Steven Givant

Introduction to Relation Algebras

Relation Algebras, Volume 1

Springer

Introduction to Relation Algebras

Steven Givant

Introduction to Relation Algebras

Relation Algebras, Volume 1

Springer

Steven Givant
Department of Mathematics
Mills College
Oakland, CA, USA

ISBN 978-3-319-65234-4 ISBN 978-3-319-65235-1 (eBook)
DOI 10.1007/978-3-319-65235-1

Library of Congress Control Number: 2017952945

Mathematics Subject Classification: 03G15, 03B20, 03C05, 03B35

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

To the memories of Alfred Tarski and Bjarni Jónsson.

Preface

The theory of relation algebras originated in the second half of the 1800s as a calculus of binary relations, in analogy with the calculus of classes (or unary relations) that was published around 1850 by George Boole in [15] and [16]. By 1900, it had developed into one of the three principal branches of mathematical logic. Yet, despite the intrinsic importance of the concepts occurring in this calculus, and their wide use and applicability throughout mathematics and science, as a mathematical discipline the subject fell into neglect after 1915.

It was revitalized and reformulated within an abstract axiomatic framework by Alfred Tarski in a seminal paper [104] from 1941, and since then the subject has grown substantially in importance and applicability. Numerous papers on relation algebras have been published since 1950, including papers in areas of computer science, and the subject has had a strong impact on such fields as universal algebra, algebraic logic, and modal logic. In particular, the study of relation algebras led directly to the development of a general theory of Boolean algebras with operators, an analogue for Boolean algebras of the well-known theory of groups with operators. This theory of Boolean algebras with operators appears to be especially well suited as an area for the application of mathematics to the theory and practice of computer science.

In my opinion, however, progress in the field and its application to other fields, and knowledge of the field among mathematicians, computer scientists, and philosophers, has been slowed substantially by the fact that, until recently, no systematic introductions to the subject existed. I believe that the appearance of such introductions will lead to a steady growth and influence of the theory and its applications, and to

a much broader appreciation of the subject. It is for this reason that I have written these two volumes: to make the basic ideas and results of the subject (in this first volume), and some of the most important advanced areas of the theory (in the second volume, *Advanced Topics in Relation Algebras*), accessible to as broad an audience as possible.

Intended audience

This two-volume textbook is aimed at people interested in the contemporary axiomatic theory of binary relations. The intended audience includes, but is not limited to, graduate students and professionals in a variety of mathematical disciplines, logicians, computer scientists, and philosophers. It may well be that others in such diverse fields such as anthropology, sociology, and economics will also be interested in the subject. Kenneth Arrow, a Nobel Prize winning economist who in 1940 took a course on the calculus of relations with Tarski, said:

> It was a great course. ...the language of relations was immediately applicable to economics. I could express my problems in those terms.

The necessary mathematical preparation for reading this work includes mathematical maturity, something like a standard undergraduate-level course in abstract algebra, an understanding of the basic laws of Boolean algebra, and some exposure to naive set theory. Modulo this background, the text is largely self-contained. The basic definitions are carefully given and the principal results are all proved in some detail.

Each chapter ends with a historical section and a substantial number of exercises. In all, there are over 900 exercises. They vary in difficulty from routine problems that help readers understand the basic definitions and theorems presented in the text, to intermediate problems that extend or enrich the material developed in the text, to difficult problems that often present important results not covered in the text. Hints and solutions to some of the exercises are available for download from the Springer book webpage.

Readers of the first volume who are mainly interested in studying various types of binary relations and the laws governing these relations might want to focus their attention on Chapters 4 and 5, which deal with the laws and special elements. Those who are more interested in the algebraic aspects of the subject might initially skip Chapters 4

and 5, referring back to them later as needed, and focus more on Chapters 1–3, which concern the fundamental notions and examples of relation algebras, and Chapters 6–13, which deal with subalgebras, homomorphisms, ideals and quotients, simple and integral relation algebras, relativizations, direct products, weak and subdirect products, and minimal relation algebras respectively.

The second volume—which consists of Chapters 14–19—deals with more advanced topics: canonical extensions, completions, representations, representation theorems, varieties and universal classes, and atom structures. Readers who are principally interested in these more advanced topics might want to skip over most of the material in Chapters 4–13, and proceed directly to the material in the second volume that is of interest to them.

Acknowledgements

I took a fascinating course from Alfred Tarski on the theory of relation algebras in 1970, and my notes for that course have served as a framework for part of the first volume. I was privileged to collaborate with him over a ten-year period, and during that period I learned a great deal more about relation algebras, about mathematics in general, and about the writing of mathematics. The monograph [113] is one of the fruits of our collaboration. Without Tarski's influence, the present two volumes would not exist.

I am very much indebted to Hajnal Andréka, Robert Goldblatt, Ian Hodkinson, Peter Jipsen, Bjarni Jónsson, Richard Kramer, Roger Maddux, Ralph McKenzie, Don Monk, and István Németi for the helpful remarks and suggestions that they provided to me in correspondence during the composition of this work. Some of these remarks are referred to in the historical sections at the end of the chapters. In particular, Hajnal Andréka, István Németi, and I have had many discussions about relation algebras that have led to a close mathematical collaboration and friendship over more than thirty years. Gunther Schmidt and Michael Winter were kind enough to provide me with references to the literature concerning applications of the theory of relation algebras to computer science.

Savannah Smith read a draft of the first volume and called many typographic errors to my attention. Kexin Liu read the second draft of both volumes, caught numerous typographic errors, and made many

suggestions for stylistic improvements. Ian Hodkinson read through the final draft of the first volume, caught several typographic errors, and made a number of very perceptive and insightful recommendations. I am very grateful to all three of them.

Loretta Bartolini an editor of the mathematical series *Graduate Texts in Mathematics*, *Undergraduate Texts in Mathematics*, and *Universitext* published by Springer, has served as the editor for these two volumes. She has given me a great deal of advice and guidance during the publication process, and I am very much indebted to her and her entire production team at Springer for pulling out all stops, and doing the best possible job in the fastest possible way, to produce these two companion volumes. Any errors or flaws that remain in the volumes are, of course, my own responsibility.

California, USA Steven Givant
July 2017

Introduction

Binary relations are a mathematical way of talking about relationships that exist between pairs of objects. Such relations permeate every aspect of mathematics, of science, and of human affairs. For example, the phrase *is a parent of* describes a binary relation that holds between two individuals a and b if and only if a is the father or the mother of b. Other examples of binary relations between human beings include the usual kinship relations such as *is an uncle of* or *is a sister of*, comparative relations such as *is richer than* or *is older than*, emotional relations such as *loves* or *is kind to*, material relations such as *owes money to* or *is a benefactor of*, and so on.

Just as there are natural operations on numbers, such as addition and multiplication, there are also natural operations on binary relations. For example, suppose F and M are the relations respectively described by the phrases *is a father of* and *is a mother of*. The union of F and M is the relation P described by the phrase *is a parent of*. The (relational) composition of F and M is the relation described by the phrase *is the maternal grandfather of*, while the composition of M and F is the relation described by the phrase *is the paternal grandmother of*. The converse of P is the relation described by the phrase *is a child of*. Thus, the operations of forming the union of two relations, the composition of two relations, and the converse of a relation are examples of operations on binary relations. Other examples include the operations of forming the intersection of two relations, the relational sum of two relations, and the complement of a relation. A set of binary relations that is closed under these operations constitutes a natural algebra of binary relations.

The operations on binary relations described in the preceding paragraph obey a great variety of laws. To give one example, let F, M, and P be the relations described above, and write B for the relation described by the phrase *is a brother of*. Suppose we first form the union $F \cup M$ of the relations F and M to obtain the relation P, and then we form the composition $B \mid P$ of B and P; the result is the relation described by the phrase *is an uncle of*. On the other hand, if we first form the compositions $B \mid F$ and $B \mid M$ to obtain the relations described by the phrases *is a paternal uncle of* and *is a maternal uncle of* respectively, and then form the union of $B \mid F$ and $B \mid M$, the result is again the relation *is an uncle of*. This state of affairs may be expressed in the form of an equation,

$$B \mid (F \cup M) = (B \mid F) \cup (B \mid M),$$

which is an instance of a law that is universally true for all binary relations, namely that the operation of forming compositions is distributive over the operation of forming unions in the sense that the composition of a relation R with the union of two relations S and T is equal to the union of the two compositions $R \mid S$ and $R \mid T$, in symbols

$$R \mid (S \cup T) = (R \mid S) \cup (R \mid T).$$

An example of a law that is not universally valid for all binary relations is the commutative law asserting that the operation of composition is commutative. Indeed, as we saw above, the composition of F and M is not the same as the composition of M and F, so the law

$$R \mid S = S \mid T$$

fails to hold for all binary relations R and S. The study of the laws that hold universally for all binary relations, that is to say, the laws that hold for all algebras of binary relations, formed an essential part of what is called the *calculus of relations* that was developed in the second half of the nineteenth century (see below).

The theory of relation algebras may be viewed as an abstract version of the calculus of relations. More precisely, it is an abstract algebraic theory of binary relations based on ten equational axioms that express laws true in all algebras of binary relations. The fundamental operations of the theory include abstract analogues of the Boolean operations of union, intersection, and complement (as applied to binary

relations), and also abstract analogues of the Peircean operations of relational addition, relational multiplication or composition, and relational converse or inverse (the latter two are analogues for binary relations of the standard operations on functions of forming compositions and inverses of functions respectively). There are distinguished constants that are abstract analogues of the empty relation, the universal relation, the identity relation, and its complement, the diversity relation. (The adjectives “Boolean” and “Peircean” respectively honor George Boole, the founder of the calculus of classes, and Charles Sanders Peirce, the founder of the calculus of relations—see below.)

The arithmetic of the theory consists of the equations and implications between equations that are derivable from the axioms. These equations and implications express basic laws that govern the behavior of the fundamental operations on binary relations, and the mutual interactions of these operations. The expressive and deductive power of this arithmetic is incomparably richer than that of Boolean algebras. Most of the standard types of binary relations that proliferate every aspect of mathematics—reflexive relations, symmetric relations, transitive relations, equivalence relations, functions, injections, surjections, bijections, permutations, squares, rectangles, partial orders, linear orders, dense linear orders without endpoints, and so on—are definable in the theory of relation algebras in the sense that abstract analogues of these relations are definable; and the basic properties of these relations are all derivable from the abstract definitions and the axioms. Regarding this richness in means of expression and proof, Alfred Tarski [104] wrote in 1941:

> It may be noticed that many laws of the calculus of relations, and in particular the axioms. . . [we have adopted] resemble theorems of the theory of groups, relative multiplication playing the role of group-theoretic composition, and the converse of a relation corresponding to the group-theoretic inverse.. . . it turns out that the calculus of relations includes the elementary theory of groups and is, so to speak, a union of Boolean algebra and group theory. This fact accounts for the deductive power and mathematical richness of the calculus.

As Tarski was to show later, even more is true: the equational theory of relation algebras provides an adequate framework for the formalization of all of classical mathematics (see below).

The equational nature of the theory of relation algebras implies that the algebraic development of the subject is based on notions that are common to other branches of algebra such as group theory, lattice the-

ory, and ring theory. These include the notions of subalgebra, homomorphism, congruence relation, quotient algebra, direct product, and subdirect product. Moreover, there are very close connections between the theory of relation algebras and several other well-known algebraic disciplines. For example, already in the early 1940s it was noticed by McKinsey (see [53]) that the algebra of complexes, or subsets, of an arbitrary group is always a relation algebra under the standard Boolean operations on subsets of the group and the Peircean operations induced on subsets by the operations of the group. The same is true of the algebra of subsets of a modular lattice with zero, as was shown by Maddux [73], and the algebra of subsets of a projective geometry, as was shown by Jónsson [49] and Lyndon [70].

Because the set of fundamental operations of a relation algebra includes the standard Boolean operations, the algebraic development of the theory of relation algebras also has close ties to algebraic and topological aspects of the theory of Boolean algebras. There are, for example, analogues for relation algebras of the various notions of complete extensions, such as canonical extensions and completions, that play such a significant role in Boolean algebra. There are important representation theorems that are analogues of Cayley's representation theorem for groups (every group is isomorphic to a group of permutations) and Stone's representation theorem for Boolean algebras (every Boolean algebra is isomorphic to a Boolean algebra of sets). In analogy with the well-known duality between Boolean algebras and Boolean topological spaces (compact, zero-dimensional, Hausdorff spaces), there are duality theorems establishing connections between relation algebras and various types of relational topological spaces (see, for example, [36]).

Finally, there are close connections to various systems of logic, including systems that are of interest to mathematicians, such as first-order logic, systems that are of interest to computer scientists, such as finite-variable logics, dynamic logics, and temporal logics, and systems that are of interest to philosophers, such as modal logics. Here are a few examples of such connections. (1) Every first-order theory of logic gives rise to a relation algebra of (congruence classes of) formulas in the same way as sentential logic gives rise to a Boolean algebra of (congruence classes of) formulas. (2) Hirsch-Hodkinson-Maddux [45] proved the following theorem about the number of variables needed to derive logically true sentences from the axioms of first-order logic, even in the case in which the sentences involved have just three variables: for every

natural number $n \geq 4$, there is a logically-true first-order sentence Γ_n with exactly three distinct variables (each occurring many times) and exactly one binary relation symbol such that any proof of Γ_n based on the axioms of first-order logic requires n distinct variables in the sense that there is a proof of Γ_n that uses n distinct variables, and Γ_n cannot be proved with fewer than n distinct variables; the original proof of this theorem was carried out within the framework of the theory of relation algebras. (3) Tarski (see [113]) proved that first-order set-theory and first-order number theory can both be formalized in a very simple version of the equational theory of relation algebras in which there are no variables, quantifiers, or sentential connectives, and in which the only rule of inference is the high school rule of replacing equals by equals. He used this result to draw a number of surprising conclusions about logical systems and the foundations of mathematics; for example, there exist undecidable subsystems of sentential logic; also, all of classical mathematics can be developed in the framework of a version of a first-order system of set theory or number theory in which there are only three variables; thus, three variables suffice for expressing and proving all classical mathematical theorems. (Note that this result does not contradict the Hirsch-Hodkinson-Maddux result mentioned in (2), because the axioms of set theory and number theory are stronger than the axioms of first-order logic.)

The theory of relation algebras soon gave rise to a more general theory of Boolean algebras with operators—an analogue of the theory of groups with operators—that was created by Jónsson and Tarski in the late 1940s (see [54] and [55]). As it turns out, a surprising number of results that are initially proved in the context of relation algebras can be generalized to much broader classes of Boolean algebras with operators.

There are numerous applications of the calculus of relations and the theory of relation algebras to various areas of computer science, some of which are detailed in such books as [95] and [19], and in the whole series of proceedings of the RelMiCS/RAMiCS (Relational Methods in Computer Science/Relational and Algebraic Methods in Computer Science) conferences from 1993 onward. For instance, there are applications to databases (see, for example, [97] and [120]), and in particular there are close connections to the database language SQL, there are applications to program development and verification (see, for example, [10] and [30]), to programming semantics (see, for example, [9], [122], [97], and [77]), and to temporal and spatial reasoning (see, for example, [29]

and [28]). There are also applications to other scientific disciplines, including anthropology (see, for example, [17] and [61]), economics (see, for example, [7] and [8]), linguistics (see, for example, [9]), social choice theory (see, for example, [7], [8], [79], and [96]), and voting theory (see, for example, [18]). For interesting applications of computer science to the study of relation algebras, see [56].

A brief history

The theory of relation algebras arose from the calculus of binary relations that was created in the second half of the nineteenth century by the English mathematician Augustus De Morgan, the American philosopher, scientist, and logician Charles Sanders Peirce, and the German mathematician Ernst Schröder as an analogue for binary relations of the calculus of classes (or unary relations) that was conceived by George Boole [15], [16], and refined by William Stanley Jevons. Concerning this early history of the subject, Tarski [104] wrote in 1941,

> The logical theory which is called the calculus of binary relations... has a strange and rather capricious line of historical development. Although some scattered remarks regarding the concept of relations are to be found already in the writings of medieval logicians, it is only with the last hundred years that this topic has become the subject of systematic investigation. The first beginnings of the contemporary theory of relations are to be found in the writings of A. De Morgan, who carried out extensive investigations in this domain in the fifties of the Nineteenth Century. De Morgan clearly recognized the inadequacy of traditional logic for the expression and justification, not merely of the more intricate arguments of mathematics and the sciences, but even of simple arguments occurring in every-day life; witness his famous aphorism, that all the logic of Aristotle does not permit us from the fact that a horse is an animal, to conclude that the head of a horse is the head of an animal. In his efforts to break the bonds of traditional logic and to expand the limits of logical inquiry, he directed his attention to the general concept of relations and fully recognized its significance. Nevertheless, De Morgan cannot be regarded as the creator of the modern theory of relations, since he did not possess an adequate apparatus for treating the subject in which he was interested, and was apparently unable to create such an apparatus. His investigations on relations show a lack of clarity and rigor which perhaps accounts for the neglect into which they fell in the following years.

> The title of creator of the theory of relations was reserved for C. S. Peirce. In several papers published between 1870 and 1882, he introduced and made precise all the fundamental concepts of the theory of relations and formulated and established its fundamental laws. Thus Peirce laid the foundation for the theory of relations as a deductive discipline; moreover he initiated the discussion of more profound problems in this domain. In particular, his investigations made it clear that a large part of the theory of relations can be presented as a calculus which is formally much like the calculus of classes developed by G. Boole and W. S. Jevons, but which greatly exceeds it in richness of expression and is therefore incomparably more interesting from the deductive point of view.
>
> Peirce's work was continued and extended in a very thorough and systematic way by E. Schröder. The latter's *Algebra und Logik der Relative*, which appeared in 1895 as the third volume of his *Vorlesungen über die Algebra der Logik*, is so far the only exhaustive account of the calculus of relations. At the same time, this book contains a wealth of unsolved problems, and seems to indicate the direction for future investigations.

By the beginning of the twentieth century, the subject had developed to the point where Bertrand Russell [92] could write in 1903:

> The subject of symbolic logic is formed by three parts: the calculus of propositions, the calculus of classes, and the calculus of relations.

The celebrated theorem of Leopold Löwenheim [65]—which is a cornerstone of modern mathematical logic, and which today would be formulated as stating that every formula valid in some model must in fact be valid in some countable model—was proved in the framework of the calculus of relations.

With the exception of Löwenheim, however, Peirce and Schröder did not have many followers. In the 1941 paper, after making the remarks quoted above, Tarski observed:

> It is therefore rather amazing that Peirce and Schröder did not have many followers. It is true that A. N. Whitehead and B. Russell, in *Principia mathematica*, included the theory of relations in the whole of logic, made this theory a central part of their logical system, and introduced many new and important concepts connected with the concept of relation. Most of these concepts do not belong, however, to the theory of relations proper but rather establish relations between this theory and other parts of logic: *Principia mathematica* contributed but slightly to the intrinsic development of the theory of relations as an independent deductive discipline. In general, it must be said that—though the significance of the theory of relations is universally recognized today—this

> theory, especially the calculus of relations, is now in practically the same stage of development as that in which it was forty-five years ago.

It was for this reason that Tarski [104] set out to revitalize and modernize the subject. He felt that there should be an axiomatic approach to the subject, a basic set of postulates from which all other laws could be derived using rules of inference. Moreover, the postulates and the methods of proof should only refer to relations, and not to other extraneous notions such as elements or pairs of elements of the universe of discourse. In other words, he imagined a presentation of the calculus of relations as an abstract algebraic discipline in much the same way as Louis Couturat and Edward Huntington had presented the Boole/Jevons calculus of classes as an abstract theory of Boolean algebras. He proposed a system of axioms—which he later simplified into ten equational axioms—and wrote that on the basis of these axioms he was practically sure he could derive all of the hundreds of laws to be found in Schröder's book. Nevertheless, he was unable to prove that every law true of all algebras of binary relations is derivable from these axioms, and so he posed this as his first problem, the completeness problem. He was also unable to show that every model of his set of axioms is isomorphic to a set relation algebra—that is to say, to an algebra of binary relations under the standard set-theoretically defined operations—and so he posed this as a second problem, the representation problem.

During the early 1940s, Tarski was able to prove that both set theory and number theory can be interpreted into a variable-free variant of his axiomatic theory of relation algebras, and therefore all of classical mathematics may be formalized within the framework of this variable-free equational theory (see [113]). On the basis of this interpretation, Tarski was also able to conclude that there is no mechanical procedure—no decision method—for establishing the truth or falsity of an equation in the theory of relation algebras. In this way, he was able to provide a concrete explanation for the observation made by Peirce regarding derivations in the calculus of relations that they "cannot be subjected to hard and fast rules like those of the Boolean calculus . . . ". Tarski pushed this result still further. He showed that his variable-free equational version of set theory can be interpreted as a finitely axiomatized subsystem of the two-valued sentential calculus. Hence, all of mathematics can be carried out within a subsystem of two-valued sentential logic.

A second phase in Tarski's work on the calculus of relations began around 1945. In that year, he held a seminar on relation algebras at the University of California at Berkeley. One portion of the seminar was devoted to a development of the arithmetic of the theory of relation algebras based on his axiom system. He and his student Louise Chin later published an important paper [23] on this subject. At the same time, Tarski attacked the completeness and representation problems with renewed energy. He focused on solving the representation problem. The first positive result was a quasi-representation theorem: every abstract relation algebra that is atomic is isomorphic to a relation algebra that is almost a set relation algebra; its universe consists of binary relations, and the basic operations of addition, relative multiplication, and converse have their set theoretic interpretation, but multiplication, relative addition, and complement do not. He showed further that if the atoms of the algebra are functions, then all of the operations have their set-theoretic interpretations, so we actually get a full representation of the abstract algebra as a set relation algebra, and not just a quasi-representation.

The quasi-representation theorem holds for atomic relation algebras, so the next logical step was to prove that every relation algebra $\mathfrak{A}$ can be extended to a complete and atomic relation algebra, the so-called the canonical (or perfect) extension of $\mathfrak{A}$. By the end of 1946 or the beginning of 1947, Tarski had succeeded in accomplishing this step, and he was also able to show that every Boolean algebra with additional unary distributive operations has a canonical extension that satisfies the same positive equations as the original algebra. He wrote about this to his former student, Bjarni Jónsson, who immediately became interested in the result, and worked to generalize it. In 1947, Jónsson succeeded in extending Tarski's theorem to classes of Boolean algebras with additional distributive operations of arbitrary ranks. In this way, the theory of Boolean algebras with operators was born—see the 1948 abstract [53], and the papers [54], and [55]. Today they play a rather important role in the applications of logic to computer science.

In the same 1948 abstract, Tarski observed that every relation algebra constructed from the complexes (or subsets) of a group is integral in the sense that it has no zero divisors with respect to the operation of relative multiplication, and he asked whether every integral relation algebra is isomorphic to an algebra of complexes of some group.

Around the end of 1948, Roger Lyndon—who had taken a course with Tarski in 1940—managed to construct a finite model of Tarski's

axioms that is not isomorphic to a set relation algebra, and he simultaneously found an example of an equational law that is true in all set relation algebras but that is not derivable from Tarski's axioms. Thus, he solved negatively both of Tarski's first two problems (see [67]). A few years later, Tarski [110] was able to prove that the class of representable relation algebras—that is to say, the class of algebras isomorphic to set relations algebras—is indeed axiomatizable by a set of equations, but this set of equations may be infinite in number. Tarski asked whether there exists a finite set of equations that axiomatizes the class.

Lyndon's results began a new chapter in the theory of relation algebras: the study of non-representable algebras. Around 1958, Jónsson, who had experienced some difficulty in understanding Lyndon's construction of a non-representable relation algebra, found a way of constructing relation algebras from projective planes. If Desargues' theorem failed in the plane, then the relation algebra constructed from the plane would not be representable. Thus, Jónsson [49] was able to construct new examples of non-representable relation algebras.

Jónsson's construction was modified and extended by Lyndon [70] to a beautiful and simple construction of relation algebras from arbitrary projective geometries. For geometries of dimension one, Lyndon's construction yields particularly simple examples of non-representable relation algebras. In the same paper, Lyndon attacked Tarski's problem concerning integral relation algebras. He was able to make some progress on it, but he was unable to solve the problem completely.

Using the relation algebras constructed by Lyndon from projective lines, Tarski's former student Donald Monk [87] was able to show around 1964 that the class of representable relation algebras is not finitely axiomatizable. Thus, any system of equations axiomatizing this class of algebras is necessarily infinite in size. A couple of years later, Monk's student Ralph McKenzie proved in [82] (see also [83]) that Tarski's problem regarding integral relation algebras also has a negative solution: there are integral relation algebras that are not isomorphic to relation algebras constructed from complexes of a group. He went further by showing that the class of integral relation algebras that are isomorphic to such group complex algebras is not finitely axiomatizable, even over the class of integral, representable relation algebras.

The impetus given to the theory of relation algebras by Tarski's reformulation of the theory and by the interesting initial problems that

he posed, the important results that were achieved in the solutions of these problems by himself and his students and grand-students Chin, Jónsson, Lyndon, Monk, and McKenzie, and the applications of these results to other domains such as computer science, have led to a revitalization of the calculus of relations in the form of the theory of relation algebras, and to the development of this subject into an active and ongoing field of research. Many new and interesting results have been obtained by scores of researchers from all parts of the globe.

We conclude this historical sketch by recalling the final sentences from Tarski's 1941 paper. They express an opinion that Tarski formed even before he obtained his major results concerning the theory of relation algebras, and it is an opinion that he kept to the end of his life.

> I do believe that the calculus of relations deserves much more attention than it receives. For, aside from the fact that the concepts occurring in this calculus possess an objective importance and are in these times almost indispensable in any scientific discussion, the calculus of relations has an intrinsic charm and beauty which makes it a source of intellectual delight to all who become acquainted with it.

Virtually everyone who has spent time working with relation algebras has learned to share Tarski's judgement.

Description and highlights of this volume

Chapter 1 describes the basic set-theoretical notions of the calculus of relations as conceived by Peirce [88]. The notion of a binary relation is introduced, examples of binary relations are given, and different ways of visualizing binary relations are presented. Some of the most common types of binary relations are discussed. The basic Boolean and Peircean operations on binary relations are defined and illustrated, and some examples of basic laws governing the behavior of these operations on binary relations are given. Boolean matrices are introduced, and the connections between the calculus of relations and the algebra of Boolean matrices are explored.

In Chapter 2, the notion of an abstract relation algebra is introduced on the basis of Tarski's ten equational axioms. The more general notion of a Boolean algebra with operators from Jónsson-Tarski [54] is defined and explored. The task of showing that a given Boolean al-

gebra with operators is in fact a relation algebra is often non-trivial, so two theorems have been included that give necessary and sufficient criteria for an atomic Boolean algebra with operators to be a relation algebra.

Chapter 3 presents some of the classic examples of relation algebras. The most important of these is the class of set relation algebras, constructed as algebras of binary relations under the set-theoretically defined operations discussed in Chapter 1. In particular, full set relation algebras, consisting of all binary relations on a given set, play a special role in the development of the subject. A rather trivial, but important class of examples of relation algebras is constructed from Boolean algebras by using Boolean operations in the role of Peircean operations. Another class of examples is constructed by using congruence classes of formulas modulo first-order theories, under operations induced by the sentential connectives and the quantifiers of the logic. A highlight of the chapter is the careful examination of three types of relation algebras that arise as complex algebras—that is to say, algebras of subsets—of specific mathematical structures, under the Boolean operations of union and complement, and with Peircean operations that are defined in terms of the fundamental notions of the structures. The examples considered are the complex algebras of groups, the complex algebras of projective geometries, and the complex algebras of modular lattices with zero. A few examples of small relation algebras that are constructed in an ad hoc fashion from finite Boolean algebras with a small number of atoms (usually less than six in number) are also given. The chapter ends with a discussion of how algebraic models similar in structure to relation algebras may be used to demonstrate the independence of Tarski's ten axioms.

Chapter 4 contains a careful development of the general arithmetic of relation algebras—that is to say, a development of the basic laws governing the behavior of the operations on binary relations—on the basis of Tarski's ten axioms. As opposed to the arithmetic of Boolean algebras in which there is just one duality principle, namely the duality between addition and multiplication, in the arithmetic of relation algebras there are three different principles of duality at work: the first is a duality between left-hand and right-hand versions of each law; the second is a duality that arises when the Boolean operations of addition and multiplication are interchanged, and simultaneously the Peircean operations of relative addition and relative multiplication are interchanged in a given law; the third is the duality that arises as the

composition of the first two dualities, that is to say, as a result of forming simultaneously the first and the second duals of a law. Thus, each law in the theory of relation algebras is closely associated with three other dual laws. The general laws of relation algebras have the flavor of a blending of laws from Boolean algebra and group theory, but their scope and content is much more complex than the laws from either Boolean algebra or group theory. For example, the semi-modular law

$$r\,;(s \mathbin{+\!\!\!,} t) \le (r\,;s) \mathbin{+\!\!\!,} t$$

(in which $;$ and $\mathbin{+\!\!\!,}$ denote the abstract binary operations of relative multiplication and relative addition respectively) expresses in a compact equational form that an existential-universal statement implies a corresponding universal-existential statement, in much the same way as uniform continuity implies continuity.

Abstract versions of many of the important types of binary relations are studied in Chapter 5. These include symmetric elements, transitive elements, equivalence elements, ideal elements of various types, rectangles, squares, functions, bijections, and permutations. For example, an element r is defined to be an equivalence element just in case

$$r^{\smile} \le r \qquad \text{and} \qquad r\,;r \le r$$

(where $^{\smile}$ denotes the operation of converse); these two inequalities respectively express in an abstract way the symmetry and transitivity of a relation denoted r. An element r is defined to be a function just in case $r^{\smile}\,;r \le 1'$ (where 1' is the identity element for relative multiplication); this inequality expresses in an abstract way that a relation denoted by r cannot map one element to two different elements. Several characterizations of each type of element are given, and the basic laws governing the behavior of the operations on these elements are established. There is a special emphasis on the distributive and modular laws that each type of element satisfies, and on the closure properties that sets of each type of element possess. For example, an element r is an equivalence element if and only if it satisfies the modular law

$$r \cdot [s\,;(r \cdot t)] = (r \cdot s)\,;(r \cdot t)$$

for all elements s and t (where $\cdot$ denotes the operation of multiplication); and r is a function if and only if it satisfies the distributive law

$$r\,;(s\cdot t)=(r\,;s)\cdot(r\,;t)$$

for all elements s and t.

Chapter 6 develops the various notions that are connected with the concept of a subalgebra—subuniverses, subalgebras, complete subalgebras, regular subalgebras, elementary subalgebras, and sets of generators—and the properties that are preserved under the passage to various types of subalgebras. The highlights of the chapter include the following theorems. The subalgebras of a relation algebra form a complete, compactly generated lattice that is closed under directed unions. The regular subalgebras of atomic relation algebras are always atomic. The Atomic Subalgebra Theorem gives sufficient conditions on a subset W of a Boolean algebra with complete operators (and in particular, on a subset of a relation algebra) $\mathfrak{A}$ for the set of sums of subsets of W to be a regular, atomic subalgebra of $\mathfrak{A}$; as an example, this theorem is applied to the study of minimal relation algebras, and it is shown that every minimal relation algebra is necessarily finite. The downward and upward Löwenheim-Skolem-Tarski Theorems guarantee the existence of elementary subalgebras and elementary extensions of specified cardinalities. Finally, the union of a system of relation algebras directed by the relation of being an elementary subalgebra is shown to be an elementary extension of each algebra in the system.

Chapter 7 develops the various notions that are connected with the concept of a homomorphism—homomorphisms, epimorphisms, monomorphisms, isomorphisms, base isomorphisms, automorphisms, complete homomorphisms, and elementary embeddings—and properties that are preserved under the passage to homomorphic images. Highlights of the chapter include the following theorems. The Atomic Isomorphism Theorem gives necessary and sufficient conditions on a bijection φ between the sets of atoms of two complete and atomic Boolean algebras with complete operators $\mathfrak{A}$ and $\mathfrak{B}$ in order for φ to extend to a uniquely determined isomorphism from $\mathfrak{A}$ to $\mathfrak{B}$. There is also an analogue for monomorphisms. A version of the Exchange Principle (also known as the Exchange Theorem) from general algebra is proved; it says that if a relation algebra $\mathfrak{A}$ is embeddable into a relation algebra $\mathfrak{B}$ with certain properties, then $\mathfrak{A}$ is actually a subalgebra of a relation algebra $\mathfrak{C}$ that is isomorphic to $\mathfrak{B}$.

The notions of a congruence, an ideal, and the quotient of a relation algebra modulo a congruence or an ideal, are treated in Chapter 8. The discussion begins with congruences and lattices of congruences

on a relation algebra, and then moves to ideals and lattices of ideals. The equivalence of the notions of a congruence and an ideal is established. It is shown that the ideals in a relation algebra form a complete, compactly generated, distributive lattice that is closed under directed unions. This theorem is followed by a discussion of the relationship between the ideals in a relation algebra $\mathfrak{A}$ and the Boolean ideals in the Boolean algebra of ideal elements in $\mathfrak{A}$. In particular, it is shown that the lattice of ideals in $\mathfrak{A}$ is isomorphic to the lattice of Boolean ideals in the Boolean algebra of ideal elements in $\mathfrak{A}$. Consequently, all of the results concerning the lattice of ideals in a relation algebra—for example, the existence of maximal ideals—may in principle be obtained as corollaries of the corresponding results for Boolean algebras.

Simple relation algebras—relation algebras in which there are exactly two ideals, the trivial ideal and the improper ideal—and integral relation algebras—non-degenerate relation algebras in which the relative product of two non-zero elements is always non-zero—are the topic of Chapter 9. A highlight of the chapter is the Simplicity Theorem, which states that, in contrast to the usual situation in, say, group theory or ring theory, the notion of simplicity for relation algebras is describable by a first-order universal sentence, and consequently every subalgebra of simple relation algebra is simple. Another important theorem says that every quantifier-free formula is equivalent to an equation in all simple relation algebras. The Integrality Theorem gives several characterizations of the notion of an integral relation algebra. One consequence of this theorem is that every integral relation algebra is simple. The chapter ends with a proof that for relation algebras, the notions of direct indecomposability, subdirect indecomposability, and simplicity all coincide.

Chapter 10 discusses the notion of the relativization of a relation algebra to an ideal element, and more generally to an equivalence element, and the properties that are preserved under the passage to relativizations. The main theorem of the chapter says that every quotient of a relation algebra $\mathfrak{A}$ modulo a principal ideal is isomorphic to a relativization of $\mathfrak{A}$ to an ideal element in $\mathfrak{A}$. Thus, quotients of $\mathfrak{A}$ modulo principal ideals have concrete representations as relativizations of $\mathfrak{A}$ and are therefore almost subalgebras of $\mathfrak{A}$ (up to isomorphisms).

The important topic of direct products and direct decompositions is treated in Chapter 11. The presentation is divided into two parts. The first part deals with the direct product of two relation algebras, and the second part with the direct product of arbitrary systems of relation al-

gebras. Two types of direct decompositions of a relation algebra $\mathfrak{A}$ are discussed: the standard notion of an external direct decomposition, in which $\mathfrak{A}$ is shown to be isomorphic to the direct product of a system of relation algebras; and the notion of an internal direct decomposition, familiar from group theory, in which $\mathfrak{A}$ is shown to be equal to the internal product of a system of relativizations of $\mathfrak{A}$ to ideal elements. It is shown that for relation algebras, the two notions are essentially equivalent. One of the highlights of the chapter is the surprising Product Decomposition Theorem, which in its binary form says that a relation algebra $\mathfrak{A}$ is the (internal) direct product of relation algebras $\mathfrak{B}$ and $\mathfrak{C}$ if and only if there is an ideal element r in $\mathfrak{A}$ such that $\mathfrak{B}$ and $\mathfrak{C}$ are equal to the relativization of $\mathfrak{A}$ to r and the relativization of $\mathfrak{A}$ to the complement of r respectively. A more general version of this theorem is given that applies to direct products of arbitrary systems of relation algebras. Another highlight of the chapter is the Total Decomposition Theorem, which says that a relation algebra $\mathfrak{A}$ has a direct decomposition into a product of simple factors if and only if the Boolean algebra of ideal elements in $\mathfrak{A}$ is atomic and has the supremum property; and furthermore, if $\mathfrak{A}$ has a direct decomposition into simple factors, then this decomposition is unique up to permutations of the factors. One consequence of this theorem is that every complete and atomic relation algebra has a unique direct decomposition into a product of simple factors. In particular, every finite relation algebra has such a unique decomposition. Another consequence is the Complete Decomposition Theorem, which says that every complete relation algebra $\mathfrak{A}$ can be written in one and only one way as the internal direct product of relation algebras $\mathfrak{B}$ and $\mathfrak{C}$, where $\mathfrak{B}$ has a unique decomposition into the direct product of simple factors, and $\mathfrak{C}$ has no simple factors whatsoever. Examples of relation algebras without any simple factors are also given.

Other types of product constructions—in particular, weak direct products, ample direct products (which are subdirect products that are intermediate between weak direct products and full direct products), and subdirect products—are dealt with in Chapter 12. As in the case of direct products, there are external and internal versions of these products; and there are characterizations, in terms of systems of ideal elements, of when a relation algebra admits a decomposition using one of these products. For example, the Weak Product Decomposition Theorem says that a relation algebra $\mathfrak{A}$ is the weak internal product of a system of relation algebras $(\mathfrak{A}_i : i \in I)$ if and only if there is a

system of ideal elements $(u_i : i \in I)$ partitioning the unit of $\mathfrak{A}$ such that the algebra $\mathfrak{A}_i$ coincides with the relativization of $\mathfrak{A}$ to u_i for each index i, and $\mathfrak{A}$ is generated by the union $\bigcup_{i\in I} A_i$ of the universes of the algebras in the system. The Semi-simplicity Theorem says that every relation algebra is isomorphic to a subdirect product of simple relation algebras. A consequence of this theorem is that an equation holds in all relation algebras if and only if it holds in all simple relation algebras.

The main goal of Chapter 13 is the classification of all minimal relation algebras. The notion of the type of a relation algebra is introduced (there are three: type one, type two, and type three), and it is shown that every simple relation algebra has a uniquely determined type. This is used to prove that the minimal simple relation algebras are, up to isomorphism, the three minimal set relation algebras $\mathfrak{M}_1$, $\mathfrak{M}_2$, and $\mathfrak{M}_3$ on sets of cardinality one, two, and three respectively. The Type Decomposition Theorem says that every relation algebra can be written as the internal product of three relation algebras of types one, two, and three respectively. The Classification Theorem for minimal relation algebras says that, up to isomorphism, there are exactly eight minimal relation algebras, namely the various possible direct products of the three minimal, simple relation algebras, with each factor occurring at most once. A more general classification theorem for relation algebras of types one and two is also given.

Chapters dependent on topics in the first volume

The material in Chapter 1 serves a motivational purpose, but it is also needed in Chapter 3 to understand two examples, set relation algebras and matrix algebras. The first of these examples plays a fundamental role throughout the two volumes, but especially in Chapters 16 and 17 in the second volume, which comprises Chapters 14–19. The remaining examples of Chapter 3 play an important role in Chapter 17.

The material in Section 2.1 is used throughout both volumes, while that of Section 2.2 is used in Chapters 6, 7, 14, 15, and 19. The material in Section 2.3 is used mainly in Chapter 3, while the logical terminology and notation of Section 2.4 is used consistently throughout both volumes, starting with Chapter 6, and that of Section 2.5 is used in one of the examples of Chapter 3 and in Chapters 16, 17, and 19.

The laws in Chapter 4 are used heavily in Chapter 5 and rather infrequently in other parts of the book. The special kinds of elements, and the laws about these elements, in Chapter 5 play a role in very specific parts of the book. Equivalence elements are needed in Chapter 10, and ideal elements are needed in Chapters 8–17. Functional elements are used in Chapter 17, rectangles in Chapter 18, and domains and ranges in Chapters 6, 9, 13, and 17.

The fundamental universal algebraic and Boolean algebraic notions (for example, the notions of a subalgebra, a regular subalgebra, a homomorphism, a complete homomorphism, an isomorphism, an ideal, quotient algebra, a simple algebra, a relativization of an algebra, and a direct product and a subdirect product of a system of algebras), and the basic results concerning these notions that are presented in various sections of Chapters 6–12 are used freely in subsequent chapters. The more specialized results in Section 6.6 are used in Chapters 7, 14, 17, and 18, while those in Section 6.8 are needed in Chapters 7, 16, 18, and 19. Similarly, the more specialized results in Section 7.6 are used in Chapters 14 and 17–19, while those in Section 7.7 are needed in Chapters 8 and 14–19, and those in Section 7.9 are needed in Chapter 18. Section 8.9 is used in Chapters 9, 11, 14, 15, and 17. The main results specific to relation algebras in Sections 9.1 and 9.2 are used in Chapters 10, 13, 14, 17, and 18, while those in Section 9.3 are needed in Chapter 11. Similarly, the main results specific to relation algebras in Section 10.4 are used in Chapters 11 and 13, while those in Section 10.5 are used in Chapters 14–16. Various of the direct product decomposition theorems for relation algebras that are given in Chapter 11 are used sporadically throughout all of the subsequent chapters of both volumes. The homomorphism decomposition theorems in Section 11.13 are used in Chapter 16. With regards to Chapter 12, only the main result of Section 12.3 is used elsewhere, namely in Chapters 13 and 16–18.

The material in the first three sections of Chapter 13 is needed in Chapter 18, while the material in the fourth section is not used again.

Contents

Chapter 1
The calculus of relations

The theory of relation algebras naturally begins with the concrete study of binary relations and operations on binary relations. This immediately raises several questions. First, what exactly is a binary relation, and how can such relations be visualized? Second, what are the natural operations on binary relations, and how can these operations be visualized? Third, what are the laws that govern the behavior of these operations, and how can the validity of these laws be established? The theory that addresses these questions is usually referred to as the *calculus of relations*. It is the task of this chapter to present a brief outline of this calculus.

1.1 Binary relations

The mathematical notion of a binary relation may be viewed as an abstraction of notions of relationships between human beings. Examples of the latter include the relation of one person being a sibling of another, the relation of one person loving another, and the relation of one person being taller than another. In mathematics, the term "relation" has a quite precise meaning that may seem, at first glance, rather distant from the colloquial meaning of the word. A (*binary*) *relation* on a set U is defined to be a subset of the set $U \times U$ of all ordered pairs (α, β) of elements α and β in U. For example, on the set U of all natural numbers, the relation of one natural number being less than another is, by definition, the set of ordered pairs (α, β) of natural numbers α and β such that $\beta = \alpha + \gamma$ for some natural number $\gamma \neq 0$. The relation of one set of natural numbers being a subset of another

S. Givant, *Introduction to Relation Algebras*,
DOI 10.1007/978-3-319-65235-1_1

is, by definition, the set of ordered pairs (X, Y) of sets X and Y of natural numbers such that, for any α, if α belongs to X, then α also belongs to Y. There are also ternary relations, that is to say, subsets of the set $U \times U \times U$ of all ordered triples of elements in U, quaternary relations, and so on, but these relations of higher rank—with a few exceptions—do not play a role in this work. Consequently, when we speak of a relation, we shall always mean a binary relation, unless explicitly stated otherwise.

Two relations R and S are defined to be *equal* if they contain the same ordered pairs. Equality may be expressed symbolically by writing

$$R = S.$$

There is also a natural inequality between relations. A relation R is said to be *less than or equal to*, or *included in*, a relation S if every pair in R also belongs to S. Inclusion may be expressed symbolically by writing

$$R \subseteq S \qquad \text{or} \qquad S \supseteq R.$$

A relation R is said to be *strictly less than*, or *properly included in*, a relation S if R is included in, but not equal to, S. Proper inclusion may be expressed symbolically by writing

$$R \subset S \qquad \text{or} \qquad S \supset R.$$

There are four natural relations that may be defined on any set U: the *empty relation* $\varnothing$ consisting of no ordered pairs, the *universal relation*

$$U \times U = \{(\alpha, \beta) : \alpha, \beta \in U\}$$

consisting of all ordered pairs of elements in U, the *identity relation*

$$id_U = \{(\alpha, \beta) : \alpha, \beta \in U \text{ and } \alpha = \beta\},$$

consisting of all pairs of equal elements in U, and the *diversity relation*

$$di_U = \{(\alpha, \beta) : \alpha, \beta \in U \text{ and } \alpha \neq \beta\}.$$

consisting of all pairs of unequal elements in U. (In the preceding equations, the notation "$\alpha, \beta \in U$" expresses that α and β are elements

of the set U.) When the set U is empty, these four relations coincide, and when U consists of a single element, the identity relation coincides with the universal relation, and the diversity relation coincides with the empty relation. When U has at least two elements, the four relations are distinct.

A relation on a set U may be visualized by using a standard coordinate system in which there is a horizontal and a vertical axis, both labeled with the elements of U. The *graph* of a relation is just a certain subset of this coordinate system. For example, if $U = \{0, 1, 2, 3, 4\}$, then the coordinate system can be visualized as a square consisting of a five-by-five array of smaller squares, each of which represents an individual ordered pair with first and second coordinates on the horizontal and vertical axes respectively. If the horizontal and vertical axes are

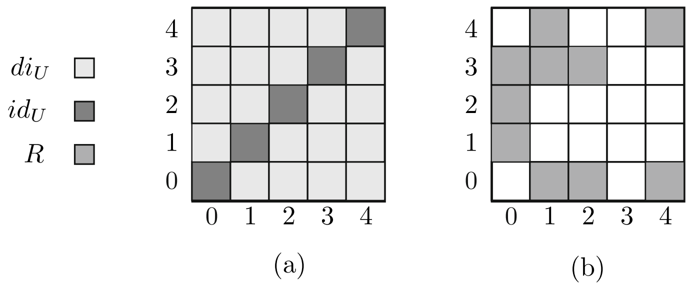


Fig. 1.1 Graphs of relations.

labeled with the numbers in U in order of increasing size, then the graph of the identity relation is the set of diagonal squares, the graph of the greater-than relation is the set of squares that are below the diagonal, the graph of the less-than relation is the set of squares that are above the diagonal, the graph of the diversity relation is the set of squares that are not on the diagonal, and the universal relation is the set of all squares—see Figure 1.1(a). The graph of the relation

$$R = \{(0,1), (0,2), (0,3), (1,0), (1,3), (1,4), (2,0), (2,3), (4,0), (4,4)\}$$

is the set of shaded squares in Figure 1.1(b). Of course, the depiction of any particular relation depends on the order in which the elements in U are placed on the two axes.

If a set U is infinite, then it is usually more convenient to represent ordered pairs not by small squares in an array, but rather by individual

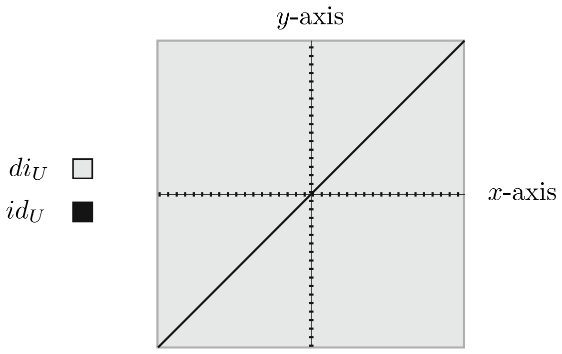


Fig. 1.2 The graphs of the identity and diversity relations on the set of real numbers.

points. For instance, if U is the set of all real numbers, then it is convenient to use the standard Cartesian coordinate system of analytic geometry to represent relations on U. In this case, the graph of the identity relation is the diagonal line defined by the equation $y = x$, the graph of the greater-than relation is the set of points below the diagonal, the graph of the less-than relation is the set of points above the diagonal, the graph of the diversity relation is the set of points not on the diagonal, and the universal relation is the set of all points—see Figure 1.2.

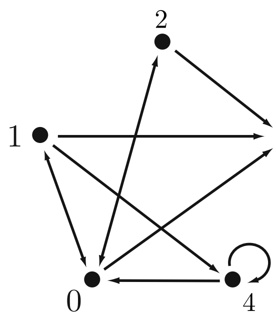


Fig. 1.3 Directed graph of the relation R from Figure 1.1(b).

Another way to visualize a relation R on a set U is as a *directed graph*. The elements in the set U are represented as the *vertices* of

the graph, and the pairs in the relation R are represented as the *directed edges* of the graph. For example, if R is the relation depicted in Figure 1.1(b), then R may be visualized as the directed graph in Figure 1.3.

1.2 Operations on relations

An *operation of rank* n on a set A is a function from the set of all n-tuples of elements in A to the set A. Thus, a *binary operation* on A is a function from $A \times A$ into A, and a *unary operation* on A is a function from A into A. A *nullary operation* on A—that is to say, an operation of rank zero—is a function whose domain consists of a single element, namely the empty set, and whose value on this element is some element in A. For this reason, nullary operations are usually identified with elements in A, and are referred to as *distinguished* (*individual*) *constants*.

For instance, suppose A is the set of integers. Addition is an example of a binary operation on A, that is to say, an operation of rank two; it correlates with every pair (α, β) of integers in $A \times A$ a unique integer γ in A that is usually denoted by $\alpha+\beta$, so that $\gamma = \alpha+\beta$. The formation of negatives is an example of a unary operation on A, that is to say, an operation of rank one; it correlates with every integer α in A a unique integer γ in A that is usually denoted by $-\alpha$, so that $\gamma = -\alpha$. The integers 0 and 1 are examples of nullary operations on A, that is to say, they are distinguished constants.

There are a number of natural operations on relations. The natural *Boolean*, or *absolute*, operations on relations are the binary operations of intersection, union, difference, and symmetric difference; and the unary operation of complement. The natural *Peircean*, or *relative*, operations on relations are the binary operations of relational multiplication, or composition, and relational addition; and the unary operation of converse, or inverse. These operations are defined as follows. If R and S are relations on a set U, then the *union* of R and S is the relation consisting of the pairs that are either in R or in S,

$$R \cup S = \{(\alpha, \beta) : (\alpha, \beta) \in R \text{ or } (\alpha, \beta) \in S\}.$$

The *intersection* of R and S is the relation consisting of the pairs that are in both R and S,

$$R \cap S = \{(\alpha, \beta) : (\alpha, \beta) \in R \text{ and } (\alpha, \beta) \in S\}.$$

The *complement* of R (with respect to the universal relation $U \times U$) is the relation consisting of the pairs that are not in R,

$${\sim}R = \{(\alpha, \beta) : (\alpha, \beta) \in U \times U \text{ and } (\alpha, \beta) \notin R\}.$$

The *difference* of R and S is the relation consisting of the pairs that are in R, but not in S,

$$R \sim S = \{(\alpha, \beta) : (\alpha, \beta) \in R \text{ and } (\alpha, \beta) \notin S\}.$$

The *symmetric difference* of R and S is the relation consisting of the pairs that are in one of R and S, but not the other,

$$R \mathbin{\triangle} S = \{(\alpha, \beta) : (\alpha, \beta) \in R \sim S \text{ or } (\alpha, \beta) \in S \sim R\}.$$

The (*relational*) *composition* of R and S is akin to the composition of two functions: it consists of the pairs (α, β) such that R "maps" α to some γ, and S "maps" γ to β,

$$R \mid S = \{(\alpha, \beta) : (\alpha, \gamma) \in R \text{ and } (\gamma, \beta) \in S \text{ for some } \gamma \in U\}.$$

The *relational sum* of R and S is a kind of logical dual of composition in the sense that "and" is replaced by "or", and the existential quantifier "for some" is replaced by the universal quantifier "for all",

$$R \dagger S = \{(\alpha, \beta) : (\alpha, \gamma) \in R \text{ or } (\gamma, \beta) \in S \text{ for all } \gamma \in U\}.$$

The (*relational*) *converse*, or *inverse*, of R is akin to the inverse of a one-to-one function: it consists of the pairs in R, but with the order of the coordinates reversed, so that if R "maps" α to β, then the converse of R "maps" β to α,

$$R^{-1} = \{(\alpha, \beta) : (\beta, \alpha) \in R\}.$$

Relational composition may be represented by a diagram such as

$$\alpha \xrightarrow{R} \gamma \xrightarrow{S} \beta.$$

Notice that this operation is not a strict analogue of functional composition, since the composition of two functions R and S is defined as

$$R \circ S = \{(\alpha, \beta) : (\alpha, \gamma) \in S \text{ and } (\gamma, \beta) \in R \text{ for some } \gamma \in U\},$$

and is usually represented by a diagram such as

$$\alpha \xrightarrow{S} \gamma \xrightarrow{R} \beta.$$

Rather, relational composition is a kind of dual of functional composition in the sense that $R \mid S = S \circ R$. (This kind of duality is different from the duality of relational addition mentioned above. We shall have more to say about the various kinds of duality in Chapter 4.)

The effects of the Boolean operations and converse on relations are easily visualized and are illustrated in Figure 1.4. For example, the graph of the converse of a relation R is just the reflection of the graph of R across the diagonal (see Figure 1.4(f)). The relational composi-

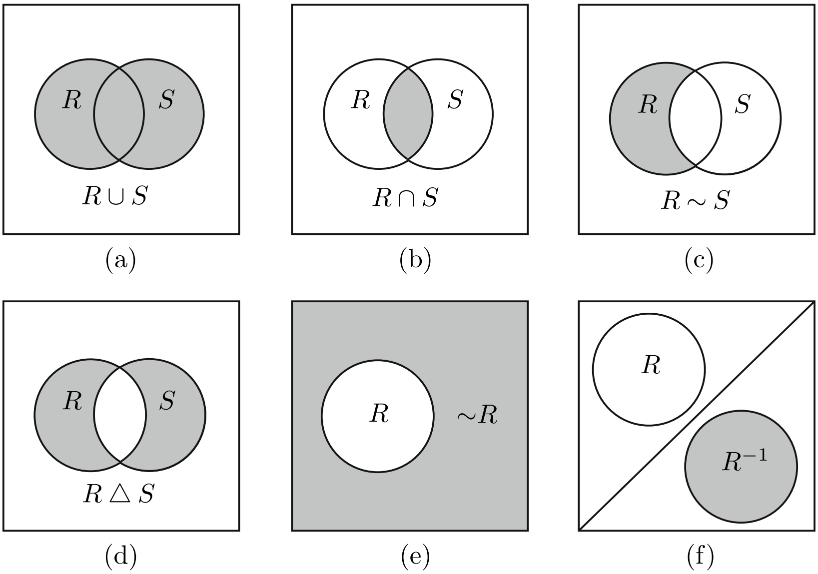


Fig. 1.4 The graphs of the union, intersection, difference, and symmetric difference of two relations R and S, and the complement and converse of a relation R.

tion and the relational sum of two relations is more complicated to

visualize. Assume for simplicity of notation that U is the set of real numbers. In order to depict relational composition, one must pass to a

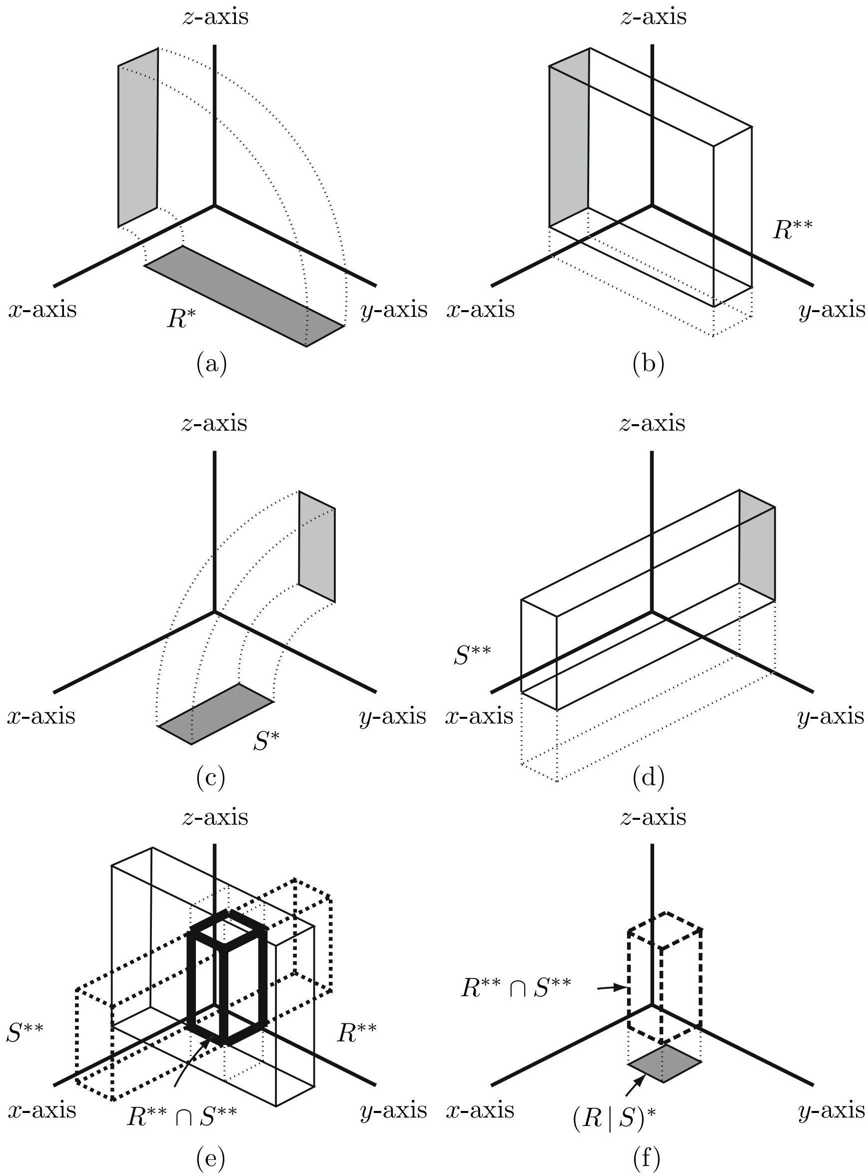


Fig. 1.5 The graph of the composition of two relations R and S.

three-dimensional coordinate system and treat the graphs of relations

as subsets of one of the planes, say the xy-plane. From an analytic perspective, this means representing each relation R as the graph of the ternary relation

$$R^* = \{(\alpha, \gamma, 0) : (\alpha, \gamma) \in R\}.$$

In order to visualize the composition of R and S, one first rotates the graph of R^* by 90° to the xz-plane to arrive at the graph of the ternary relation

$$\{(\alpha, 0, \gamma) : (\alpha, \gamma) \in R\}$$

(see Figure 1.5(a)), and then forms the cylinder

$$R^{**} = \{(\alpha, \delta, \gamma) : (\alpha, \gamma) \in R \text{ and } \delta \in U\}$$

in the direction of the y-axis with the rotated graph of R^* as its base (see Figure 1.5(b)). Similarly, one rotates the graph of

$$S^* = \{(\gamma, \beta, 0) : (\gamma, \beta) \in S\}$$

by 90° onto the yz-plane to arrive at the graph of the ternary relation

$$\{(0, \beta, \gamma) : (\gamma, \beta) \in S\}$$

(see Figure 1.5(c)), and then forms the cylinder

$$S^{**} = \{(\xi, \beta, \gamma) : (\gamma, \beta) \in S \text{ and } \xi \in U\}$$

in the direction of the x-axis with the rotated graph of S^* as its base (see Figure 1.5(d)). One then intersects the two cylinders to obtain the graph of

$$R^{**} \cap S^{**} = \{(\alpha, \beta, \gamma) : (\alpha, \gamma) \in R \text{ and } (\gamma, \beta) \in S\}$$

(see Figure 1.5(e)) and projects the result onto the xy-plane to arrive at the graph of the ternary relation that represents the composition of R and S (see Figure 1.5(f)),

$$(R \,|\, S)^* = \{(\alpha, \beta, 0) : (\alpha, \gamma) \in R \text{ and } (\gamma, \beta) \in S \text{ for some } \gamma \in U\}.$$

We shall follow the usual conventions regarding the order in which operations are to be performed when parentheses are omitted: unary operations take precedence over binary operations, and among binary

operations, multiplications take precedence over additions and subtractions. For example, $R \cap S^{-1}$ is to be understood as $R \cap (S^{-1})$, and $R \mid S \cup T$ is to be understood as $(R \mid S) \cup T$.

Some of the operations on relations that are discussed above are definable in terms of the others. For example, intersection and difference can be defined in terms of union and complement as follows:

$$R \cap S = {\sim}({\sim}R \cup {\sim}S) \qquad \text{and} \qquad R \sim S = R \cap {\sim}S = {\sim}({\sim}R \cup S).$$

Similarly, relational addition can be defined in terms of composition and complement:

$$R \dagger S = {\sim}({\sim}R \mid {\sim}S).$$

The empty relation, the universal relation, and the diversity relation can all be defined in terms of the identity relation, using the operations of union and complement:

$$\varnothing = {\sim}({\sim}id_U \cup id_U), \qquad U \times U = {\sim}id_U \cup id_U, \qquad di_U = {\sim}id_U.$$

Consequently, in a formal development of calculus of relations, it is convenient to select union, complement, composition, converse, and the identity relation as the primitive notions, and to define the remaining notions in terms of them.

1.3 Relational laws

A primary concern of the calculus of relations in its original form was the study of laws that govern operations on relations. Many of the most important laws have the form of equations. Examples include the *associative laws* for (relational) composition and relational addition,

$$R \mid (S \mid T) = (R \mid S) \mid T, \qquad R \dagger (S \dagger T) = (R \dagger S) \dagger T,$$

the right- and left-hand *identity laws* for composition and relational addition,

$$R \mid id_U = R = id_U \mid R, \qquad R \dagger di_U = R = di_U \dagger R,$$

the *first* and *second involution laws*,

$$(R^{-1})^{-1} = R, \qquad (R \mid S)^{-1} = S^{-1} \mid R^{-1},$$

the right- and left-hand *distributive laws* for composition over union,

$$(R \cup S) \mid T = (R \mid T) \cup (S \mid T), \qquad T \mid (R \cup S) = (T \mid R) \cup (T \mid S),$$

and relational addition over intersection,

$$(R \cap S) \dagger T = (R \dagger T) \cap (S \dagger T), \qquad T \dagger (R \cap S) = (T \dagger R) \cap (T \dagger S),$$

and the *distributive laws* for converse over union and intersection,

$$(R \cup S)^{-1} = R^{-1} \cup S^{-1}, \qquad (R \cap S)^{-1} = R^{-1} \cap S^{-1}.$$

Each of these laws can be established by a straightforward set theoretic argument. For example, here is a set-theoretic derivation of the second involution law. For any elements α and β in the universe U, each of the following statements is equivalent to its neighbors:

$$\begin{aligned}
&(\alpha, \beta) \in (R \mid S)^{-1}, \\
&(\beta, \alpha) \in R \mid S, \\
&(\beta, \gamma) \in R \text{ and } (\gamma, \alpha) \in S \text{ for some } \gamma \in U\ , \\
&(\alpha, \gamma) \in S^{-1} \text{ and } (\gamma, \beta) \in R^{-1} \text{ for some } \gamma \in U, \\
&(\alpha, \beta) \in S^{-1} \mid R^{-1},
\end{aligned}$$

by the definitions of the operations of converse and composition.

Some laws have the form of equivalences between equations. For example, the *De Morgan-Tarski laws* state that

$$\begin{aligned}
(R \mid S) \cap T = \varnothing \qquad &\text{if and only if} \qquad (R^{-1} \mid T) \cap S = \varnothing, \\
&\text{if and only if} \qquad (T \mid S^{-1}) \cap R = \varnothing.
\end{aligned}$$

As in the case of equational laws, equivalences can usually be established by straightforward set-theoretic arguments. For example, the first of the De Morgan-Tarski laws follows from the equivalence of each of the following assertions to its neighbors, where α, β, and γ are arbitrary elements in the universe U:

$(R \,|\, S) \cap T = \varnothing$,
for all α, β, either $(\alpha, \beta) \notin R \,|\, S$ or $(\alpha, \beta) \notin T$,
for all α, β, γ, either $(\alpha, \gamma) \notin R$ or $(\gamma, \beta) \notin S$ or $(\alpha, \beta) \notin T$,
for all γ, β, α, either $(\alpha, \gamma) \notin R$ or $(\alpha, \beta) \notin T$ or $(\gamma, \beta) \notin S$,
for all γ, β, α, either $(\gamma, \alpha) \notin R^{-1}$ or $(\alpha, \beta) \notin T$ or $(\gamma, \beta) \notin S$,
for all γ, β, either $(\gamma, \beta) \notin R^{-1} \,|\, T$ or $(\gamma, \beta) \notin S$,
$(R^{-1} \,|\, T) \cap S = \varnothing$,

by the definitions of the operations of intersection, composition, and converse, and the definition of the empty relation.

Many important laws take the form of inequalities. Examples include the inequalities

$$id_U \subseteq R \dagger {\sim}(R^{-1}), \qquad R \,|\, {\sim}(R^{-1}) \subseteq di_U,$$

and

$$(R \dagger S) \,|\, T \subseteq R \dagger (S \,|\, T), \qquad R \,|\, (S \dagger T) \subseteq (R \,|\, S) \dagger T.$$

Notice that every inequality can be expressed as an equation, since

$$R \subseteq S \qquad \text{if and only if} \quad R \cup S = S.$$

Consequently, an inequality can always be treated as an equation, and in fact we shall often refer to inequalities as equations.

Inequalities may be established by means of the same kinds of set-theoretical arguments that apply to equations. For example, to establish the first inequality above, observe that a pair (γ, β) of elements from U belongs to the relation ${\sim}(R^{-1})$ just in case the pair (β, γ) does not belong to R. Consequently, a pair (α, β) of elements from U belongs to the right side of the inequality just in case for all elements γ in U, either (α, γ) is in R or (β, γ) is not in R, by the definition of relational addition. If (α, β) belongs to the left side of the inequality, then $\alpha = \beta$; and since (α, γ) either is, or is not, in R, no matter what γ is, it follows that (α, β) belongs to the right side of the inequality.

1.4 Relational properties

A number of important properties that a (binary) relation may possess can be expressed very simply and neatly within the calculus of relations, without any references to elements, by means of equations (and

inequalities) using the operations on relations defined in Section 1.2. In this section, we shall give a few examples to illustrate the general ideas.

The property of a relation R on a set U being *reflexive*, that is to say, the property that the pair (α, α) is in R for every element α in U, is expressed by the inclusion $id_U \subseteq R$. Similarly, the property of a relation R being *symmetric*, that is to say, the property

$$(\alpha, \beta) \in R \qquad \text{implies} \qquad (\beta, \alpha) \in R,$$

is expressed by the inclusion $R^{-1} \subseteq R$. The property of a relation R being *transitive*, that is to say, the property

$$(\alpha, \gamma) \in R \qquad \text{and} \qquad (\gamma, \beta) \in R \qquad \text{implies} \qquad (\alpha, \beta) \in R,$$

is expressed by the inclusion $R \,|\, R \subseteq R$. These observations may be combined to conclude that R is an equivalence relation on the set U, that is to say, a reflexive, symmetric, and transitive relation on U, if and only if it satisfies the inequality

$$id_U \cup R^{-1} \cup (R \,|\, R) \subseteq R,$$

or, equivalently, if and only if it satisfies the equation

$$id_U \cup (R \,|\, R^{-1}) = R.$$

Just as the notions associated with equivalence relations are expressible in terms of equations (and inequalities), so too are the notions associated with partial orders. For example, the property of a relation R on a set U being *anti-symmetric*, that is to say,

$$(\alpha, \beta) \in R \qquad \text{and} \qquad (\beta, \alpha) \in R \qquad \text{implies} \qquad \alpha = \beta,$$

is expressed by the inequality

$$R \cap R^{-1} \subseteq id_U.$$

It follows that R is a *partial order* on the set U, that is to say, a reflexive, anti-symmetric, and transitive relation on U, if and only if it satisfies the equation

$$[(id_U \cup (R \,|\, R)) \sim R] \cup [(R \cap R^{-1}) \sim id_U] = \varnothing.$$

Indeed, the preceding equation is true just in case each of the two equations

$$(id_U \cup (R \mid R)) \sim R = \varnothing \qquad \text{and} \qquad (R \cap R^{-1}) \sim id_U = \varnothing$$

is true, and these two equations respectively express the inclusions

$$id_U \cup (R \mid R) \subseteq R \qquad \text{and} \qquad R \cap R^{-1} \subseteq id_U .$$

The standard notions associated with functions are also expressible by means of equations in the calculus of relations. For example, a relation R on a set U is a *function*, that is to say,

$$(\alpha, \beta) \in R \qquad \text{and} \qquad (\alpha, \gamma) \in R \qquad \text{implies} \qquad \beta = \gamma,$$

just in case R satisfies the inequality

$$R^{-1} \mid R \subseteq id_U .$$

A function R is a *one-to-one*, that is to say,

$$(\alpha, \gamma) \in R \qquad \text{and} \qquad (\beta, \gamma) \in R \qquad \text{implies} \qquad \alpha = \beta,$$

just in case it satisfies the inequality

$$R \mid R^{-1} \subseteq id_U .$$

The *domain* of the relation R, that is to say, the set of left-hand coordinates of the pairs in R, is the entire set U just in case R satisfies the equation

$$R \mid (U \times U) = U \times U ,$$

and the *range* of R, that is to say, the set of right-hand coordinates of the pairs in R, is the entire set U just in case R satisfies the equation

$$(U \times U) \mid R = U \times U .$$

As the preceding remarks imply, there is a way of talking about sets within the calculus of relations, without referring to elements. Indeed, an element α belongs to the domain, respectively the range, of an arbitrary relation R on a set U just in case the pair (α, α) belongs to the

relation $R\,|(U\times U)$, respectively the relation $(U\times U)\,|\,R$. Consequently, the relations

$$(R\,|(U\times U))\cap id_U \qquad \text{and} \qquad ((U\times U)\,|\,R)\cap id_U$$

can be used to talk about the domain and range of R.

Properties of finite sequences of relations may also be equationally expressible. For example, two relations R and S on a set U are said to be *conjugated quasi-projections* on U if they are functions with the property that, for any two elements α and β in U, there is always an element γ in U such that

$$(\gamma,\alpha)\in R \qquad \text{and} \qquad (\gamma,\beta)\in S.$$

If one thinks of the element γ as encoding the ordered pair (α,β), then the relations R and S may be viewed as the left- and right-projection functions that map each ordered pair to its left- and right-coordinate respectively. The property of relations R and S being conjugated quasi-projections on U is expressible in the calculus of relations by the equation

$$[\sim[(R^{-1}\,|\,R)\cup(S^{-1}\,|\,S)]\cup id_U]\cap(R^{-1}\,|\,S)=U\times U.$$

Indeed, the preceding equation is true just in case each of the equations

$$\sim[(R^{-1}\,|\,R)\cup(S^{-1}\,|\,S)]\cup id_U=U\times U \qquad \text{and} \qquad R^{-1}\,|\,S=U\times U$$

is true. The first of these two equations expresses that the relations $R^{-1}\,|\,R$ and $S^{-1}\,|\,S$ are both included in id_U, or put a different way, the complement of the union of these two relations includes the diversity relation. In other words, the first equation expresses that R and S are both functions. The second equation expresses that, being functions, R and S possess the characteristic property of conjugated quasi-projections.

Conjugated quasi-projections play a crucial role in establishing one of the most important metamathematical applications of the calculus of relations. Though it is far from obvious, it turns out that all of mathematics may be formalized in a variable-free version of the calculus of relations. This version contains no variables, quantifiers, or sentential connectives of any kind; its only formulas are equations between relational terms, and its only rule of inference is the high school rule of replacing equals by equals. Yet this highly simplified formal

system suffices for the development of all of classical mathematics. In particular, variables, quantifiers, and sentential connectives may be dispensed with in the development of classical mathematics. See the article Givant [35], which may also be found at

doi:10.1007/s10817-006-9062-x,

for more extensive remarks about this result.

In view of the observations made above, it is natural to ask which properties of relations or of systems of relations are expressible by means of equations in the calculus of relations. The rather surprising answer is that precisely those properties are expressible that can be defined in the first-order language of relations (see Section 2.5) using at most three distinct variables (and no individual constant symbols). If a pair of conjugated quasi-projections is available, then every first-order definable property of relations and systems of relations (with no restriction on the number of variables) can be expressed in the calculus of relations. Again, see the article cited above for more details.

1.5 Boolean matrices

There is a very interesting and illuminating connection between binary relations and Boolean matrices. In this section we discuss these matrices and the natural operations on them, and in the next section we explore the connections between relations and matrices.

Some preliminary remarks about the two-element Boolean algebra are in order. The universe of this algebra is the set consisting of the numbers 0 and 1. Following traditional set-theoretic notation, this set is denoted by 2, so that

$$2 = \{0, 1\}.$$

Binary operations of addition $+$ and multiplication $\cdot$, and a unary operation of complement $-$ are defined on this universe in Table 1.1. Multiplication is definable in terms of addition and complement by the equation

$$r \cdot s = -[(-r) + (-s)], \tag{1}$$

so it is often omitted from the list of fundamental operations on 2.

For every set V, we can form the Boolean algebra that is the Vth *direct power* of 2. Its universe is the set 2^V consisting of all functions

$+$	0	1
0	0	1
1	1	1

,

$\cdot$	0	1
0	0	0
1	0	1

,

	$-$
0	1
1	0

Table 1.1 Addition, multiplication, and complement tables for the two-element Boolean algebra.

whose domain is V and whose range is included in 2. For instance, if V is the set

$$3 = \{0, 1, 2\},$$

then there are eight such functions, two examples of which are the functions M and N defined in Table 1.2.

r	$M(r)$
0	1
1	1
2	0

,

r	$N(r)$
0	1
1	0
2	0

Table 1.2 Functions M and N in 2^3.

The operations of addition, multiplication, and complement on 2 induce corresponding operations on 2^V that are defined coordinatewise. For example, the sum of functions M and N in 2^V is the function L in 2^V defined by

$$L(\alpha) = M(\alpha) + N(\alpha)$$

for every element α in V, where the addition on the right is performed in 2. The product of M and N, and the complement of M, are defined in an analogous fashion. The same symbols are used to denote addition, multiplication, and complement on 2^V as are used to denote the corresponding operations on 2. For example, $M + N$ denotes the sum of functions M and N in 2^V. In this notation, the preceding definition of addition assumes the form

$$(M + N)(\alpha) = M(\alpha) + N(\alpha).$$

The context will always make clear whether the symbol being used denotes an operation on 2 (as on the right side of the preceding equation) or the corresponding operation on 2^V (as on the left side of the equation). For a concrete example, take M and N to be the functions

in 2^3 defined in Table 1.2. The sum $M+N$ is the function in 2^3 defined by

$$
\begin{aligned}
(M+N)(0) &= M(0)+N(0) = 1+1 = 1,\\
(M+N)(1) &= M(1)+N(1) = 1+0 = 1,\\
(M+N)(2) &= M(2)+N(2) = 0+0 = 0,
\end{aligned}
$$

while the complement $-M$ is the function in 2^3 defined by

$$
\begin{aligned}
(-M)(0) &= -(M(0)) = -1 = 0,\\
(-M)(1) &= -(M(1)) = -1 = 0,\\
(-M)(2) &= -(M(2)) = -0 = 1.
\end{aligned}
$$

Fix a set U, and take V to be the Cartesian product

$$V = U \times U.$$

The functions from $U \times U$ into 2, that is to say, the elements of the set

$$2^V = 2^{U \times U}$$

are called *U-by-U Boolean matrices*, or simply *matrices* for short. To represent such a matrix M in the traditional fashion as a square array, consider the case when U is the set

$$n = \{0, 1, 2, \ldots, n-1\}.$$

Number the rows of the array from 0 to $n-1$, with row 0 at the top and row $n-1$ at the bottom, and number the columns from 0 to $n-1$, with column 0 on the left and column $n-1$ on the right. For each pair of indices α and β between 0 and $n-1$, the $\alpha\beta$th *entry* of the array, that is to say, the entry in the αth row and the βth column of the array, is $M(\alpha, \beta)$ (see Table 1.3). For example, the matrices on the set

$$3 = \{0, 1, 2\}$$

may be represented as 3-by-3 arrays, and there are

$$2^{3 \cdot 3} = 2^9 = 512$$

of them. Two concrete examples of such matrices are

	0	1	2	$\ldots$	β	$\ldots$	$n-1$
0	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$
1	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$
2	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$
$\vdots$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$
α	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$M(\alpha,\beta)$	$\cdot$	$\cdot$
$\vdots$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$
$n-1$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$	$\cdot$

Table 1.3 Form of an $n \times n$ matrix.

$$M = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \qquad \text{and} \qquad N = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}. \tag{2}$$

There are certain distinguished matrices, namely the *zero matrix*, whose entries are all 0, the *unit matrix*, whose entries are all 1, the *identity matrix*, whose $\alpha\beta$th entry is 1 when $\alpha = \beta$, and 0 when $\alpha \neq \beta$, and the *diversity matrix*, whose $\alpha\beta$th entry is 0 when $\alpha = \beta$, and 1 when $\alpha \neq \beta$. In the case when U is the set 3, these matrices have the forms

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

respectively.

The definitions of the operations of (Boolean) addition and complement, defined above on 2^V for an arbitrary set V, assume the form

$$(M+N)(\alpha,\beta) = M(\alpha,\beta) + N(\alpha,\beta),$$
$$(-M)(\alpha,\beta) = -(M(\alpha,\beta))$$

for U-by-U matrices. These are just the traditional linear algebraic definitions of the operations of forming the sum of two matrices and the negative of a matrix (except that the operations on the right sides of the definitions are the Boolean operations on 2, not the standard operations of forming sums and negatives of real or complex numbers).

For example, suppose M and N are 3-by-3 matrices in which the entries in, say, row 1 are m_{10}, m_{11}, m_{12}, and n_{10}, n_{11}, n_{12} respectively, then the entries in row 1 of the sum matrix $M+N$ are

$$m_{10} + n_{10}, \qquad m_{11} + n_{11}, \qquad m_{12} + n_{12},$$

and the entries in row 1 of the complement matrix $-M$ are

$$-m_{10}, \qquad -m_{11}, \qquad -m_{12}.$$

For a concrete example in the case of 3-by-3 matrices, take M and N to be the matrices defined in (2). The sum $M + N$ and the complement $-M$ are the 3-by-3 matrices determined by

$$M + N = \begin{pmatrix} 1+1 & 0+1 & 1+0 \\ 0+1 & 0+0 & 1+1 \\ 1+0 & 1+1 & 0+1 \end{pmatrix} = \begin{pmatrix} 1\,1\,1 \\ 1\,0\,1 \\ 1\,1\,1 \end{pmatrix}$$

and

$$-M = \begin{pmatrix} -1 & -0 & -1 \\ -0 & -0 & -1 \\ -1 & -1 & -0 \end{pmatrix} = \begin{pmatrix} 0\,1\,0 \\ 1\,1\,0 \\ 0\,0\,1 \end{pmatrix}.$$

The operation of (Boolean) multiplication on matrices is defined in a similar manner, but this operation does not have a traditional analogue in linear algebra. Notice that, for matrices, multiplication is definable in terms of addition and complement by the equation in (2), just as in the case of the two-element Boolean algebra.

There are two non-Boolean operations on U-by-U matrices that are suggested by the analogy with traditional matrices in linear algebra, namely the binary operation of *matrix multiplication* and unary operation of *matrix transposition*. The *matrix product* of two U-by-U matrices M and N is the U-by-U matrix L defined by

$$L(\alpha, \beta) = \textstyle\sum_{\gamma \in U} M(\alpha, \gamma) \cdot N(\gamma, \beta)$$

for every pair of elements α and β in U, where the sums and products on the right are formed in the two-element Boolean algebra. We use the symbol $\odot$ to denote the operation of matrix multiplication, so that $L = M \odot N$.

For instance, suppose M and N are 3-by-3 matrices. If the entries in, say, row 1 of M are m_{10}, m_{11}, m_{12}, and if the entries in, say, column 2 of N are n_{02}, n_{12}, n_{22}, then the entry in row 1 and column 2 of the matrix product $M \odot N$ is

$$m_{10} \cdot n_{02} + m_{11} \cdot n_{12} + m_{12} \cdot n_{22}.$$

For a concrete example in the case of 3-by-3 matrices, let M and N be the matrices defined in (2); then

$$M \odot N = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} \odot \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix},$$

where the third matrix is obtained from the first two by means of the following computation:

$$\begin{pmatrix} 1\cdot 1 + 0\cdot 1 + 1\cdot 0 & 1\cdot 1 + 0\cdot 0 + 1\cdot 1 & 1\cdot 0 + 0\cdot 1 + 1\cdot 1 \\ 0\cdot 1 + 0\cdot 1 + 1\cdot 0 & 0\cdot 1 + 0\cdot 0 + 1\cdot 1 & 0\cdot 0 + 0\cdot 1 + 1\cdot 1 \\ 1\cdot 1 + 1\cdot 1 + 0\cdot 0 & 1\cdot 1 + 1\cdot 0 + 0\cdot 1 & 1\cdot 0 + 1\cdot 1 + 0\cdot 1 \end{pmatrix}$$

The *transpose* of a U-by-U matrix M is the U-by-U matrix L defined by

$$L(\alpha, \beta) = M(\beta, \alpha)$$

for every pair of elements α and β in U. We use the traditional superscript T to denote the operation of matrix transposition, so that $L = M^{\mathrm{T}}$.

For instance, if M is a 3-by-3 matrix in which the entries in, say, row 2 are the values m_{20}, m_{21}, m_{22}, then these values become the entries in column 2 of the transpose matrix M^{T}. For a concrete example of matrix transposition, take M to be the 3-by-3 matrix with zeros above the diagonal and ones everywhere else; then

$$M^{\mathrm{T}} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}^{\mathrm{T}} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

As has already been pointed out, the matrix operation of Boolean multiplication does not have an analogue within the traditional theory of matrices, but in the theory of Boolean matrices it plays an important role, in part because it is the dual operation of Boolean addition in the sense of equation (1). There is an analogous situation for the operation of matrix multiplication on Boolean matrices: corresponding to this operation, there is a dual operation of matrix addition that does not have an analogue within the traditional theory of matrices. The definition of this operation is obtained by interchanging the role of addition and multiplication in the definition of matrix multiplication.

In more detail, the *matrix sum* of two U-by-U matrices M and N is the U-by-U matrix L defined by

$$L(\alpha, \beta) = \prod_{\gamma \in U}(M(\alpha, \gamma) + N(\gamma, \beta))$$

for every pair of elements α and β in U, where the products and sums on the right are formed in the two-element Boolean algebra. We use the symbol $\oplus$ to denote the operation of matrix addition, so that $L = M \oplus N$.

For instance, suppose M and N are 3-by-3 matrices. If the entries in, say, row 1 of M are m_{10}, m_{11}, m_{12}, and if the entries in, say, column 2 of N are n_{02}, n_{12}, n_{22}, then the entry in row 1 and column 2 of the matrix sum $M \oplus N$ is

$$(m_{10} + n_{02}) \cdot (m_{11} + n_{12}) \cdot (m_{12} + n_{22}).$$

For a concrete example in the case of 3-by-3 matrices, let M and N be the matrices defined in (2); then

$$M \oplus N = \begin{pmatrix} 1\,0\,1 \\ 0\,0\,1 \\ 1\,1\,0 \end{pmatrix} \oplus \begin{pmatrix} 1\,1\,0 \\ 1\,0\,1 \\ 0\,1\,1 \end{pmatrix} = \begin{pmatrix} 1\,0\,1 \\ 1\,0\,0 \\ 0\,1\,1 \end{pmatrix},$$

where the third matrix is obtained from the first two by means of the following computation:

$$\begin{pmatrix} (1+1)\cdot(0+1)\cdot(1+0) & (1+1)\cdot(0+0)\cdot(1+1) & (1+0)\cdot(0+1)\cdot(1+1) \\ (0+1)\cdot(0+1)\cdot(1+0) & (0+1)\cdot(0+0)\cdot(1+1) & (0+0)\cdot(0+1)\cdot(1+1) \\ (1+1)\cdot(1+1)\cdot(0+0) & (1+1)\cdot(1+0)\cdot(0+1) & (1+0)\cdot(1+1)\cdot(0+1) \end{pmatrix}$$

Matrix addition is definable in terms of matrix multiplication and complement by the equation

$$M \oplus N = -((-M) \odot (-N)),$$

so it is often omitted from the list of fundamental matrix operations. Notice the very close analogy between this equation and the equation in (1).

1.6 Relations and Boolean matrices

The similarity between the calculus of relations and the calculus of Boolean matrices goes beyond simple analogy; they are really two sides

of the same coin. Every relation has a corresponding matrix, and every matrix has a corresponding relation, and this correspondence is bijective in nature and preserves all operations. Here are the details.

A relation on a set U is a subset of the Cartesian product $U \times U$. With each such relation R, we may associate a U-by-U matrix M_R that is defined by

$$M_R(\alpha, \beta) = \begin{cases} 1 & \text{if} \quad (\alpha, \beta) \in R\,, \\ 0 & \text{if} \quad (\alpha, \beta) \notin R\,, \end{cases}$$

for all α and β in U. For example, if R is the relation

$$R = \{(0,0), (0,2), (1,2), (2,1), (2,2)\}$$

on the set $U = 3$, then

$$M_R = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

Similarly, with every U-by-U matrix M, we may associate a relation R_M on U that is defined by

$$(\alpha, \beta) \in R_M \qquad \text{if and only if} \qquad M(\alpha, \beta) = 1.$$

For example, if M is the 3-by-3 matrix

$$M = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix},$$

then

$$R_M = \{(0,0), (0,1), (0,2), (1,1), (1,2), (2,0), (2,2)\}.$$

Start with a relation R, pass to the corresponding matrix M_R, and then pass to the relation corresponding to the matrix M_R; the definitions of the correspondence given above make clear that the result is the original relation R. Similarly, start with a matrix M, pass to the corresponding relation R_M, and then pass to the matrix corresponding to the relation R_M; the result is the original matrix M. This state of affairs may be summarized by saying that the function mapping each relation R on U to the U-by-U matrix M_R is a bijection from the set

of relations on U to the set of U-by-U matrices, and the inverse of this bijection is the function that maps each U-by-U matrix M to the relation R_M on U.

The correspondence between relations on a set U and U-by-U matrices maps the empty relation, the universal relation, the identity relation, and the diversity relation to the zero matrix, the unit matrix, the identity matrix, and the diversity matrix respectively. Moreover, the correspondence preserves operations in the sense that for any relations R, S, and T on U,

$$T = R \cup S \qquad \text{if and only if} \qquad M_T = M_R + M_S, \tag{1}$$
$$T = R \cap S \qquad \text{if and only if} \qquad M_T = M_R \cdot M_S, \tag{2}$$
$$T = {\sim}R \qquad \text{if and only if} \qquad M_T = -M_R, \tag{3}$$
$$T = R \dagger S \qquad \text{if and only if} \qquad M_T = M_R \oplus M_S, \tag{4}$$
$$T = R \mid S \qquad \text{if and only if} \qquad M_T = M_R \odot M_S, \tag{5}$$
$$T = R^{-1} \qquad \text{if and only if} \qquad M_T = (M_R)^{\mathrm{T}}. \tag{6}$$

For example, to establish (1), observe that for any elements α and β in U,

$$\begin{aligned} (\alpha,\beta) \in R \cup S \qquad &\text{if and only if} \qquad (\alpha,\beta) \in R \text{ or } (\alpha,\beta) \in S, \\ &\text{if and only if} \qquad M_R(\alpha,\beta) = 1 \text{ or } M_S(\alpha,\beta) = 1, \\ &\text{if and only if} \qquad M_R(\alpha,\beta) + M_S(\alpha,\beta) = 1, \\ &\text{if and only if} \qquad (M_R + M_S)(\alpha,\beta)) = 1, \end{aligned}$$

by the definition of the union of two relations, the definition of the matrix corresponding to a relation, the definition of addition in 2, and the definition of the sum of two matrices. Thus,

$$(\alpha,\beta) \in R \cup S \qquad \text{if and only if} \qquad (M_R + M_S)(\alpha,\beta) = 1. \tag{7}$$

Also,

$$(\alpha,\beta) \in T \qquad \text{if and only if} \qquad M_T(\alpha,\beta) = 1, \tag{8}$$

by the definition of the matrix corresponding to a relation. The definition of relational equality implies that

$$\begin{aligned} &T = R \cup S \quad \text{just in case, for all } \alpha \text{ and } \beta \text{ in } U, \\ &\qquad\qquad (\alpha,\beta) \in T \quad \text{if and only if} \quad (\alpha,\beta) \in R \cup S. \end{aligned} \tag{9}$$

Similarly, the definition of matrix equality implies that

$$M_T = M_R + M_S \quad \text{just in case, for all } \alpha \text{ and } \beta \text{ in } U,$$
$$M_T(\alpha,\beta) = 1 \quad \text{if and only if} \quad (M_R + M_S)(\alpha,\beta) = 1. \tag{10}$$

Use (7) and (8) to replace

$$(\alpha,\beta) \in R \cup S \qquad \text{and} \qquad (\alpha,\beta) \in T$$

in (9) with

$$(M_R + M_S)(\alpha,\beta) = 1 \qquad \text{and} \qquad M_T(\alpha,\beta) = 1$$

respectively, and combine the result with (10), to arrive at (1).

To give one more example, here is the derivation of (5). Observe that for any elements α and β in U, each of the following assertions is equivalent to its neighbor:

$$\begin{aligned}
&(\alpha,\beta) \in R\,|\,S,\\
&(\alpha,\gamma) \in R \quad \text{and} \quad (\gamma,\beta) \in S \quad \text{for some } \gamma \in U,\\
&M_R(\alpha,\gamma) = 1 \quad \text{and} \quad M_S(\gamma,\beta) = 1 \quad \text{for some } \gamma \in U,\\
&M_R(\alpha,\gamma) \cdot M_S(\gamma,\beta) = 1 \quad \text{for some } \gamma \in U,\\
&\textstyle\sum_{\gamma\in U} M_R(\alpha,\gamma) \cdot M_S(\gamma,\beta) = 1,\\
&(M_R \odot M_S)(\alpha,\beta) = 1.
\end{aligned}$$

The first equivalence uses the definition of relational composition, the second uses the definition of the matrix corresponding to a relation, the third uses the definition of multiplication in 2, the fourth uses the definition of addition in 2, and the fifth uses the definition of matrix multiplication. Thus,

$$(\alpha,\beta) \in R\,|\,S \qquad \text{if and only if} \qquad (M_R \odot M_S)(\alpha,\beta) = 1. \tag{11}$$

The definition of relational equality implies that

$$T = R\,|\,S \quad \text{just in case, for all } \alpha \text{ and } \beta \text{ in } U,$$
$$(\alpha,\beta) \in T \quad \text{if and only if} \quad (\alpha,\beta) \in R\,|\,S. \tag{13}$$

Similarly, the definition of matrix equality implies that

$$M_T = M_R \odot M_S \quad \text{just in case, for all } \alpha \text{ and } \beta \text{ in } U,$$
$$M_T(\alpha,\beta) = 1 \quad \text{if and only if} \quad (M_R \odot M_S)(\alpha,\beta) = 1. \tag{14}$$

Use (11) and (8) to replace

$$(\alpha,\beta) \in R \,|\, S \qquad \text{and} \qquad (\alpha,\beta) \in T$$

in (13) with

$$(M_R \odot M_S)(\alpha,\beta) = 1 \qquad \text{and} \qquad M_T(\alpha,\beta) = 1$$

respectively, and combine the result with (14), to arrive at (5).

The reader may have noticed a similarity between the matrix representation of a relation R and the graphical representation of R as described in Section 1.1. In fact, if we place the horizontal axis (labeled in order of increasing size, as is traditional) at the top of the graph, instead of at the bottom in the traditional way, and if we label the vertical axis (placed on the left, as is traditional) from the top to the bottom of the graph in order of increasing size, instead of from the bottom to the top in the traditional way, then the graph representing the relation R has a filled-in square at exactly those places where the matrix representing R has a 1. For example, if R is the relation

$$R = \{(0,1),(0,2),(0,3),(1,0),(1,3),(1,4),(2,0),(2,3),(4,0),(4,4)\}$$

that is illustrated by the graph in Figure 1.1(b), then in this non-

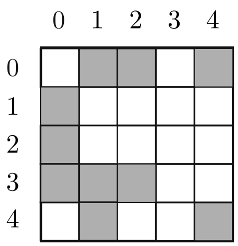


Fig. 1.6 Graph of the relation R with the axes presented in a different way.

traditional way of placing and labeling the axes, the graph of R assumes the form given in Figure 1.6, while the matrix representation of R assumes the form

$$M_R = \begin{pmatrix} 0&1&1&0&1 \\ 1&0&0&0&0 \\ 1&0&0&0&0 \\ 1&1&1&0&0 \\ 0&1&0&0&1 \end{pmatrix}.$$

Observe that the graph representing R in Figure 1.6 has a filled-in square at the same places where matrix M_R has a 1.

The preceding discussion shows that the calculus of relations and the calculus of Boolean matrices really amount to the same thing. The latter provides a different perspective on the former, one that is very closely tied to the traditional theory of matrices in linear algebra. It may seem surprising at first that matrices are just another way of looking at relations, and that the standard matrix operations are all analogues of standard operations on relations; in particular, matrix multiplication is the analogue of relational composition. A moment's reflection, however, reveals that the same situation exists in linear algebra: matrices are just another way of looking at linear transformations, and the standard matrix operations are all analogues of standard operations on linear transformations; in particular, matrix multiplication is the analogue of the operation of composition on linear transformations.

1.7 Historical remarks

The development of the calculus of relations is due primarily to Augustus De Morgan [26], Charles Sanders Peirce—see in particular [88]—and Friedrich Wilhelm Karl Ernst Schröder [98]. Concerning this development, Alfred Tarski [104] wrote the remarks quoted in the historical section of the introduction to the present volume.

The definition of the notion of a binary relation as a set of ordered pairs dates back to Schröder [98]. The Boolean operations on relations are particular cases of the more general operations on sets that were first studied by George Boole and William Stanley Jevons. De Morgan [26] appears to have been the first to investigate certain other natural operations on relations (albeit in a verbal form), including the binary operation of composition and the unary operations of converse and of converse-complement; and he formulated various laws regarding these operations. It was Peirce (see [88]) who, after

much experimentation, arrived at the final set of fundamental operations on binary relations, and the distinguished binary relations, that form the foundation of the theory of relations today. Peirce also formulated many of the important basic laws that these operations and distinguished relations obey, including all of the laws mentioned in Section 1.3 except the De Morgan-Tarski laws. The latter go back to equivalences that were studied by De Morgan; in their present form they are due to Tarski.

Interest in the expressive power of the calculus of relations dates back at least to Schröder [98]. In particular, explicit equations expressing properties such as transitivity, functionality, and one-to-oneness are given in [98]. Schröder also recognized that unary relations, or sets, could be discussed within the framework of the calculus of relations. The problem of characterizing the properties of relations that are expressible in the calculus of relations dates back to Schröder as well; he seems to have believed that all first-order properties of relations are so expressible (see pp. 550–551 of [98]). The first example showing that not every first-order property of relations is expressible in the calculus of relations was found by Korselt and published in Löwenheim [65]. Tarski [104] sharpened Korselt's negative result, and later proved that a property of relations or sequences of relations is expressible in the calculus of relations if and only if it is definable in the first-order theory of relations using at most three variables (see [113]). The notion of a conjugated quasi-projection is due to Tarski. He used these relations to prove that first-order set-theory, and hence all of classical mathematics, can be formalized in a variable-free (equational) version of the calculus of relations (see [113]). For more historical information on the early history of the calculus of relations, see Lewis [63] and Maddux [76].

The interpretation of relations as Boolean matrices, and the interpretation of operations on relations as operations on matrices, is due to Schröder [98] (see, in particular, pp. 43–57 of that work).

Abstract formulations of the observations in Exercises 1.13–1.18 below are due to Tarski (see [23]).

Exercises

1.1. Let R be the relation on the set

$$U = \{0, 1, 2, 3, 4, 5\}$$

that is defined by

$$R = \{(0,0), (0,1), (0,2), (0,3), (1,3), (2,0), (2,4), (3,0), (3,1), (3,5), (4,0), (4,4), (5,0), (5,1), (5,3)\}.$$

Draw a picture of R analogous to the one in Figure 1.1(b), and then draw a directed graph that represents R, as in Figure 1.3.

1.2. List the ordered pairs in the equivalence relation on the set

$$U = \{0, 1, 2, 3, 4, 5\}$$

whose equivalence classes are $\{0, 1, 2\}$, $\{3\}$, and $\{4, 5\}$. Draw a picture of this relation analogous to the one in Figure 1.1(b), and then draw a directed graph that represents this relation, as in Figure 1.3.

1.3. List the ordered pairs in the relation on the set

$$U = \{0, 1, 2, 3, 4, 5\}$$

that holds between two numbers α and β just in case α is congruent to $\beta + 3$ modulo 6. Draw a picture of this relation analogous to the one in Figure 1.1(b), and then draw a directed graph that represents this relation, as in Figure 1.3.

1.4. Consider the set A of all (binary) relations on a given set U. For each binary operation O on A defined below, describe the set of ordered pairs that belong to the relation $O(R, S)$ in terms of the ordered pairs that belong to the given relations R and S in A, and then give a geometric description of $O(R, S)$ in terms of R and S.

(i) The operation O of *implication*, defined by

$$O(R, S) = {\sim}R \cup S.$$

(ii) The operation O of *equivalence*, defined by

$$O(R, S) = (R \cap S) \cup ({\sim}R \cap {\sim}S).$$

(iii) The operation O defined by

$$O(R, S) = R \cap S^{-1}.$$

(iv) The operation O defined by

$$O(R,S) = R \mid S^{-1}.$$

1.5. Consider the set A of all relations on a given set U. For each unary operation O on A defined below, describe the set of ordered pairs that belong to the relation $O(R)$ in terms of the ordered pairs that belong to the given relation R, and then give a geometric description of $O(R)$ in terms of R.

(i) The operation O of *converse-complement*, defined by

$$O(R) = {\sim}(R^{-1}).$$

(ii) The operation O defined by

$$O(R) = R \,|(U \times U).$$

(iii) The operation O defined by

$$O(R) = (U \times U) \mid R.$$

(iv) The operation O defined by

$$O(R) = (U \times U) \mid R \,|(U \times U)$$

(v) The operation O defined by

$$O(R) = R \dagger \varnothing.$$

(vi) The operation O defined by

$$O(R) = \varnothing \dagger R.$$

(vii) The operation O defined by

$$O(R) = R \dagger {\sim}(R^{-1}).$$

1.6. Prove that the relational sum of two finite relations on an infinite set is always empty.

1.7. A relation on the set of real numbers is said to be *bounded* if its graph is entirely included in some circle of finite radius. Prove that the relational sum of two bounded relations on the set of real numbers is always empty.

1.8. Give a geometric interpretation of the relational sum of two relations R and S.

1.9. If the graphs of R and S are circles in the real plane, what is the graph of the composition $R \mid S$?

1.10. Prove that the following laws are valid for any relations R and S on a set U.

(i) $R \cap S = {\sim}({\sim}R \cup {\sim}S)$.
(ii) $R \sim S = R \cap {\sim}S = {\sim}({\sim}R \cup S)$.
(iii) $R \dagger S = {\sim}({\sim}R \mid {\sim}S)$.
(iv) $\varnothing = {\sim}({\sim}id_U \cup id_U)$.
(v) $U \times U = {\sim}id_U \cup id_U$.
(vi) $di_U = {\sim}id_U$.

1.11. Prove that the following laws are valid.

(i) The associative law for relational composition.
(ii) The associative law for relational addition.
(iii) The identity laws for relational composition.
(iv) The identity laws for relational addition.
(v) The first involution law.
(vi) The distributive laws for relational composition over union.
(vii) The distributive laws for relational addition over intersection.
(viii) The distributive law for converse over union.
(ix) The distributive law for converse over intersection.
(x) The second of the De Morgan-Tarski laws.

1.12. Prove that each of the following inequalities is valid.

(i) $id_U \subseteq R \dagger {\sim}(R^{-1})$.
(ii) $R \mid {\sim}(R^{-1}) \subseteq di_U$.
(iii) $(R \dagger S) \mid T \subseteq R \dagger (S \mid T)$.
(iv) $R \mid (S \dagger T) \subseteq (R \mid S) \dagger T$.

1.13. Prove that a relation R on a set U is symmetric and transitive if and only if it satisfies the equation $R \mid R^{-1} = R$. Conclude that R is an equivalence relation on U if and only if R satisfies the equation

$$id_U \cup (R \mid R^{-1}) = R.$$

1.14. Prove that an equivalence relation R on a non-empty set U has exactly two equivalence classes or at least three equivalence classes respectively, according to whether the equation

$$(\sim R) \,|\, (\sim R) = R \qquad \text{or} \qquad (\sim R) \,|\, (\sim R) = U \times U$$

is valid.

1.15. Let R be an equivalence relation on a set U with at least three elements. Prove that the equations

$$\begin{aligned}
&(R \cap di_U) \,|\, (R \cap di_U) = \varnothing, \\
&(R \cap di_U) \,|\, (R \cap di_U) = R \cap id_U, \\
&(R \cap di_U) \,|\, (R \cap di_U) = R
\end{aligned}$$

respectively express that every equivalence class of R has exactly one element, exactly two elements, or at least three elements.

1.16. Prove that if a relation R on a set U is symmetric and transitive, then so is the relation $\sim R \,|\, \sim R$.

1.17. Suppose S is a relation on a set U, and $R = S \,|\, (U \times U)$. Prove that $R \,|\, R = R$.

1.18. Prove that a relation R on a set U is a function if and only if

$$(R \,|\, di_U) \dagger \varnothing = \varnothing.$$

1.19. If R and S are functions on a set U, prove that $R \,|\, S$ is also a function.

1.20. In Section 1.5, it was observed that multiplication in the two-element Boolean algebra is definable in terms of addition and complement. Show that, conversely, addition is definable in terms of multiplication and complement.

1.21. Given tables for each of the eight functions from the set 3 into the set 2. Choose two of these functions, and write tables for the sum, product, and complements of your two functions.

1.22. How many 2-by-2 Boolean matrices are there? List them all using matrix notation.

1.23. How many 4-by-4 Boolean matrices are there? Give the zero matrix, the unit matrix, the identity matrix, diversity matrix, and two other 4-by-4 matrices of your choice.

1.24. If M and N are the 3-by-3 matrices

$$M = \begin{pmatrix} m_{00} & m_{01} & m_{02} \\ m_{10} & m_{11} & m_{12} \\ m_{20} & m_{21} & m_{22} \end{pmatrix} \qquad \text{and} \qquad N = \begin{pmatrix} n_{00} & n_{01} & n_{02} \\ n_{10} & n_{11} & n_{12} \\ n_{20} & n_{21} & n_{22} \end{pmatrix},$$

write out formulas in matrix notation for each of the following matrices.

(i) $M + N$.
(ii) $M \cdot N$.
(iii) $-M$.
(iv) $M \oplus N$.
(v) $M \odot N$.
(vi) M^{T}.

1.25. If M and N are the 3-by-3 matrices

$$M = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \qquad \text{and} \qquad N = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},$$

write each of the following matrices using matrix notation.

(i) $M + N$.
(ii) $M \cdot N$.
(iii) $-M$.
(iv) $M \oplus N$.
(v) $M \odot N$.
(vi) M^{T}.

1.26. If R is the relation on the set $3 = \{0, 1, 2\}$ given by

$$R = \{(0, 1), (1, 0), (1, 2), (2, 0), (2, 1)\},$$

what is the corresponding matrix M_R?

1.27. If R is the relation on the set $4 = \{0, 1, 2, 3\}$ given by

$$R = \{(0, 0), (0, 2), (1, 0), (1, 3), (2, 0), (2, 3), (3, 1), (3, 2)\},$$

what is the corresponding matrix M_R?

1.28. If M is the 3-by-3 matrix

$$M = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix},$$

what is the corresponding relation R_M?

1.29. If M is the 4-by-4 matrix

$$M = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix},$$

what is the corresponding relation R_M?

1.30. Prove equivalences (2), (3), (4), and (6) in Section 1.6.

Chapter 2
Relation algebras

The theory of relation algebras is an abstract algebraic version of the calculus of relations that was outlined in Chapter 1. There are four new components to the theory. First, ten simple laws from the calculus of relations have been singled out as axioms of the theory; in particular, the theory is axiomatic in nature. Second, each of the axioms has the form of an equation, and the only rules of inference that are permitted are the rule of substitution and the rule of replacement of equals by equals, both familiar from high school algebra. Derivations of laws are therefore no longer set-theoretical arguments in which one shows that a pair of elements from the universe belongs to the relation on one side of an equation if and only if it belongs to the relation on the other side; rather, they are equational derivations from the ten axioms. Third, the equational setting implies that one can apply standard algebraic methods—such as the formation of homomorphic images, direct products, and subalgebras—to analyze the models of the theory, that is to say, to analyze relation algebras, and to construct new relation algebras from old ones. This leads to a rich algebraic theory that is similar in spirit to the algebraic theories of groups (an abstraction of the theory of permutations), rings (an abstraction of the theory of polynomials), and Boolean algebras (an abstraction of the calculus of classes). Fourth, although the intended models of the theory are algebras of relations (to be defined in Chapter 3), there are other kinds of algebras in which the axioms of the theory are all valid. This generality leads to a variety of beautiful and unexpected models, and to interconnections with other important mathematical domains such as group theory and projective geometry. It also leads to a host of interesting questions that otherwise would not arise.

S. Givant, *Introduction to Relation Algebras*,
DOI 10.1007/978-3-319-65235-1_2

2.1 Fundamental notions and axioms

The notion of a relation algebra is a special case of a more general notion of algebra from the theory of general algebraic structures. An *algebra* is a system consisting of a non-empty set called the *universe* of the algebra, and a family of operations on the universe. These operations are called the *fundamental operations* of the algebra.

Definition 2.1. A *relation algebra* is an algebra

$$\mathfrak{A} = (A\,,\,+\,,\,-\,,\,;\,,\,{}^{\smile}\,,\,1\text{'}\,)$$

in which $+$ and $;$ are binary operations on the universe A, while $-$ and ${}^{\smile}$ are unary operations on A, and 1' is a distinguished constant of A, such that the following axioms are satisfied for all elements r, s, and t in A.

(R1) $r + s = s + r$.
(R2) $r + (s + t) = (r + s) + t$.
(R3) $-(-r + s) + -(-r + -s) = r$.
(R4) $r\,;(s\,;t) = (r\,;s)\,;t$.
(R5) $r\,;1\text{'} = r$.
(R6) $r^{\smile\smile} = r$.
(R7) $(r\,;s)^{\smile} = s^{\smile}\,;r^{\smile}$.
(R8) $(r + s)\,;t = r\,;t + s\,;t$.
(R9) $(r + s)^{\smile} = r^{\smile} + s^{\smile}$.
(R10) $r^{\smile}\,;-(r\,;s) + -s = -s$.

The set A is called the *universe* of $\mathfrak{A}$. The *Boolean* operations $+$ and $-$ are called (*Boolean*) *addition* and *complement* (or *complementation*) respectively. The *Peircean* operations $;$ and ${}^{\smile}$ are called *relative multiplication* and *converse* (or *conversion*) respectively. The distinguished Peircean constant 1' is called the *identity element.* □

The axioms in the preceding definition are commonly referred to using the following names: (R1) is the *commutative law for addition*, (R2) is the *associative law for addition*, (R3) is *Huntington's law*, (R4) is the *associative law for relative multiplication*, (R5) is the (right-hand) *identity law for relative multiplication*, (R6) is the *first involution law*, (R7) is the *second involution law*, (R8) is the (right-hand) *distributive law for relative multiplication*, (R9) is the *distributive law for converse*, and (R10) is *Tarski's law.*

As the notation of the preceding definition implies, we shall use upper case (German) fraktur letters to refer to relation algebras (and, much later on, to relational structures). When referring to other algebraic or geometric structures such as groups, Boolean algebras, or projective geometries, we shall usually use the upper case italic letter that denotes the universe of the structure. This will simplify the notation and make it more readable. We shall adopt one more simplification of notation. In order to distinguish carefully between the operations of different relation algebras $\mathfrak{A}$ and $\mathfrak{B}$, one should employ different notations to distinguish the operations of the two algebras, for example, by using superscripts such as

$$\mathfrak{A} = (A\,,\, +^{\mathfrak{A}}\,,\, -^{\mathfrak{A}}\,,\, ;^{\mathfrak{A}}\,,\, {}^{\smile\mathfrak{A}}\,,\, 1\text{'}^{\mathfrak{A}}\,)$$

In practice, the context usually makes clear when the operation symbols in question refer to the operations of $\mathfrak{A}$ and when they refer to the operations of $\mathfrak{B}$; so we shall always omit such superscripts when no confusion can arise.

It is common practice in algebra to identify the universe of an algebra with the algebra itself, therefore to speak of algebra as if one were speaking of universe, and vice versa. We shall follow this practice to a certain extent. For example, we shall often speak about elements in $\mathfrak{A}$ and subsets of $\mathfrak{A}$, instead of elements in, and subsets of, the universe of $\mathfrak{A}$. We shall also speak about the *cardinality* of $\mathfrak{A}$, by which is meant the cardinality, or size, of the universe of $\mathfrak{A}$.

The conventions regarding the order in which operations are to be performed when parentheses are omitted are the same as those mentioned in Section 1.2 for the calculus of relations: unary operations take precedence over binary operations, and among binary operations, multiplications take precedence over additions and subtractions. For example, in fully parenthesized form, Axioms (R7), (R8), and (R10) might be written as

$$(r\,;s)^{\smile} = (s^{\smile})\,;(r^{\smile}), \qquad (r+s)\,;t = (r\,;t) + (s\,;t),$$

and

$$((r^{\smile})\,;(-(r\,;s))) + (-s) = -s.$$

Axioms (R1)–(R3) imply that the *Boolean part* of a relation algebra $\mathfrak{A}$, namely the algebra $(A\,,\,+\,,\,-)$, is a Boolean algebra. In particular, the notions and laws from the theory of Boolean algebras apply

to relation algebras. For example, the binary operations of (*Boolean*) *multiplication*, *difference* or *subtraction*, and *symmetric difference* are respectively defined by

$$r \cdot s = -(-r + -s), \quad r - s = r \cdot -s, \quad r \ominus s = (r - s) + (s - r)$$

for all r and s in $\mathfrak{A}$. The dual use of the symbol $-$ to denote the unary operation of complement, and the binary operation of Boolean difference should cause no confusion. The same dual use of this symbol occurs in the arithmetic of the integers. The context always makes clear whether the unary or the binary operation is intended. Regarding the order of operations when parentheses are omitted, multiplications take precedence over differences. For example, $r\,;s - r\,;t$ is to be understood as $(r\,;s) - (r\,;t)$. The Boolean constants *zero* and *one* (or the *unit*) are respectively defined by

$$0 = -(-1' + 1') \qquad \text{and} \qquad 1 = -1' + 1'.$$

Note that when the terms "addition" and "multiplication", or their analogues "sum" and "product", are used without any modifier, they refer to the Boolean operations and not the Peircean operations, unless the context makes another intention clear.

It is well known and easy to check that the operation $\ominus$ of symmetric difference is associative and commutative in the sense that the equations

$$r \ominus (s \ominus t) = (r \ominus s) \ominus t \qquad \text{and} \qquad r \ominus s = s \ominus r$$

always hold. Zero is the identity element for this operation because

$$r \ominus 0 = 0 \ominus r = r,$$

and every element is its own inverse with respect to this operation because $r \ominus r = 0$. Conclusion: the elements of a relation algebra form a Boolean group (that is to say, a group in which each element is its own inverse) under the operation of symmetric difference.

A *partial order* $\leq$ is defined on the universe of a relation algebra by

$$r \leq s \quad \text{if and only if} \quad r + s = s.$$

This definition makes clear that every inequality $r \leq s$ may be viewed as an equation, namely the equation $r + s = s$ (or, equivalently, the equation $r \cdot s = r$). We write $r < s$ if $r \leq s$ and $r \neq s$.

The *sum*, or *supremum*, of a set X of elements in a relation algebra is defined to be the least upper bound of X, provided such a least upper bound exists. In other words, r is the supremum of X if r is an upper bound for X in the sense that $s \leq r$ for every s in X, and if r is below every other upper bound t of X in the sense that $r \leq t$. Of course, the supremum of an infinite set of elements may not exist. The *product*, or *infimum*, of the set X is defined to be the greatest lower bound of X, provided such a greatest lower bound exists. In other words, r is the infimum of X if r is a lower bound for X in the sense that $r \leq s$ for every s in X, and if r is above every other lower bound t of X in the sense that $t \leq r$. We shall denote the sum and product of X, when they exist, by $\sum X$ and $\prod X$ respectively. Notice that if X is a finite set, say

$$X = \{r_0, \ldots, r_{n-1}\},$$

then

$$\sum X = r_0 + \cdots + r_{n-1} \qquad \text{and} \qquad \prod X = r_0 \cdot \ \cdots \ \cdot r_{n-1}.$$

The sum of a system of elements $(r_i : i \in I)$ is defined to be the supremum of the set $\{r_i : i \in I\}$. We shall write $\sum_{i \in I} r_i$ to denote this sum (when it exists), and if the context makes clear what index set I is intended, then we shall often omit any reference to it and write simply $\sum_i r_i$, or even just $\sum r_i$. Analogous remarks apply to the product of a system of elements.

The supremum of the empty subset is, by convention, 0. Indeed, 0 is an upper bound of the empty subset (it is vacuously above every element in the empty set), and it is obviously the least such upper bound. Similarly, the infimum of the empty subset is, by convention, 1. Indeed, 1 is a lower bound of the empty subset (it is vacuously below every element in the empty set), and it is obviously the greatest such lower bound.

A relation algebra is said to be *complete* if every subset of the universe has a supremum and an infimum. As with Boolean algebras, it suffices to require the existence of the supremum of every subset; the existence of the infimum of every subset then follows easily. A relation algebra is said to be *countably complete*, or *σ-complete*, if every countable subset of the universe has a supremum and an infimum. Again, it suffices to require the existence of the supremum of every countable subset; the existence of the infimum of every countable subset then follows.

An *atom* in a relation algebra is defined to be a minimal, non-zero element. In other words, r is an atom if $r \neq 0$, and if $s \leq r$ always implies that either $s = 0$ or $s = r$. A relation algebra is said to be *atomic* if every non-zero element is above an atom, and *atomless* if it contains no atoms at all. Warning: the relation algebra with just one element in its universe, namely zero, is both atomic and atomless. It is called the *degenerate* relation algebra. A non-degenerate relation algebra may be atomic, or atomless, or neither. However, a finite relation algebra is necessarily atomic, and therefore a non-degenerate atomless relation algebra is necessarily infinite.

Two elements r and s in a relation algebra are said to be *disjoint* if their product $r \cdot s$ is 0. More generally, a set of elements is said to be disjoint if any two distinct elements in the set are disjoint. Similarly, a system $(r_i : i \in I)$ of elements is called disjoint if $i \neq j$ always implies that r_i and r_j are disjoint. A *partition* of an element r is a disjoint set, or system, of elements that has r as its supremum. With a few exceptions (that will be explicitly pointed out), it is always assumed that the elements in a partition are all non-zero.

A *Boolean homomorphism* from a relation algebra $\mathfrak{A}$ to a relation algebra $\mathfrak{B}$ is a mapping φ from the universe of $\mathfrak{A}$ to the universe of $\mathfrak{B}$ that preserves the Boolean operations of addition and complement in the sense that

$$\varphi(r+s) = \varphi(r) + \varphi(s) \qquad \text{and} \qquad \varphi(-r) = -\varphi(r)$$

for all elements r and s in $\mathfrak{A}$. It is easy to check that a Boolean homomorphism must also preserve the defined operations of multiplication, subtraction, and symmetric difference, and it must map zero and one to zero and one respectively. If a Boolean homomorphism φ is one-to-one, or onto, or both, then φ is called a Boolean *monomorphism*, *epimorphism*, or *isomorphism* respectively. A Boolean isomorphism that maps $\mathfrak{A}$ to itself is called a Boolean *automorphism* of $\mathfrak{A}$.

Axioms (R4)–(R7) imply that the *Peircean part* of a relation algebra $\mathfrak{A}$, namely the algebra $(A\,,\,;\,,\,{}^{\smile}\,,\,1')$, is a monoid with involution. In other words, it is a semigroup under the operation $\,;\,$, with an identity element 1', and with a unary operation ${}^{\smile}$ that satisfies the two involution laws. In this respect, the Peircean part of a relation algebra is somewhat similar in nature to a group (which is also a monoid with an involution). In relation algebras, however, elements do not in general have inverses with respect to the operation of relative multiplication. Nevertheless, the arithmetic of relation algebras is a curious

and fascinating blend of the laws of Boolean algebra and of group theory. The distributivity axioms (R8) and (R9) ensure that a relation algebra is a Boolean algebra with operators (see below), so the entire theory of Boolean algebras with operators can be applied to relation algebras.

A binary Peircean operation $\mathbin{+\!\!\!,}$ of *relative addition* and a distinguished Peircean constant 0' called the *diversity element* are defined by

$$r \mathbin{+\!\!\!,} s = -(-r \mathbin{;} -s) \qquad \text{and} \qquad 0\text{'} = -1\text{'}$$

respectively.

Tarski's law, that is to say, Axiom (R10), is the real workhorse of the theory, and most of the important laws are directly or indirectly derived with its help. It is clear from the definition of the partial order $\leq$ that (R10) is just an equational form of the inequality

$$r^{\smile} \mathbin{;} -(r \mathbin{;} s) \leq -s.$$

In the presence of (R1)–(R3) and (R6)–(R9), this inequality is equivalent to the implication

$$\text{if} \quad (r \mathbin{;} s) \cdot t = 0, \quad \text{then} \quad (r^{\smile} \mathbin{;} t) \cdot s = 0 \tag{R11}$$

(the details are left as an exercise). In fact, in the presence of the other axioms, (R10) is equivalent to the following *De Morgan-Tarski laws*:

$$\begin{aligned} (r \mathbin{;} s) \cdot t = 0 \qquad & \text{if and only if} \qquad & (r^{\smile} \mathbin{;} t) \cdot s = 0, \\ & \text{if and only if} \qquad & (t \mathbin{;} s^{\smile}) \cdot r = 0, \\ & \text{if and only if} \qquad & (s^{\smile} \mathbin{;} r^{\smile}) \cdot t^{\smile} = 0, \\ & \text{if and only if} \qquad & (t^{\smile} \mathbin{;} r) \cdot s^{\smile} = 0, \\ & \text{if and only if} \qquad & (s \mathbin{;} t^{\smile}) \cdot r^{\smile} = 0 \end{aligned}$$

(see Lemma 4.8 and Corollary 4.9). As one passes from one of these equations to another, the variables are permuted in a cyclic fashion. For this reason, the De Morgan-Tarski laws are sometimes called the cycle laws. We shall use the term *cycle law* to refer to (R11) alone.

2.2 Boolean algebras with operators

A number of the deepest and most important results about relation algebras hold for a much broader class of algebras called Boolean al-

gebras with operators. In this section, we take a preliminary look at these algebras.

Consider an arbitrary Boolean algebra $(A\,,+\,,-)$. A binary operation $\,;\,$ on the universe A is said to be *distributive* (over addition), or *additive*, if it is distributive in each argument in the sense that for any elements r, s, and t in A,

$$r\,;(s+t) = r\,;s + r\,;t \qquad \text{and} \qquad (r+s)\,;t = r\,;t + s\,;t.$$

The operation is said to satisfy the *general finite distributivity law* (over addition) if for all finite, non-empty subsets X and Y of A,

$$(\sum X)\,;(\sum Y) = \sum\{r\,;s : r \in X \text{ and } s \in Y\}$$

It is a straightforward matter to extend the preceding definitions to operations on A of arbitrary rank $n > 0$. A word about terminology: when speaking of the distributivity of an operation, we shall always mean its distributivity over addition, unless explicitly stated otherwise.

Lemma 2.2. *An operation on a Boolean algebra is distributive if and only if it satisfies the general finite distributivity law.*

Proof. Obviously, an operation that satisfies the general finite distributivity law must be distributive (in each argument). To establish the reverse implication, consider the case of a binary distributive operation $\,;\,$. A straightforward argument by induction on natural numbers $n > 0$ shows that

$$p\,;(s_0 + \cdots + s_{n-1}) = p\,;s_0 + \cdots + p\,;s_{n-1}, \tag{1}$$

$$(r_0 + \cdots + r_{n-1})\,;q = r_0\,;q + \cdots + r_{n-1}\,;q, \tag{2}$$

whenever the elements involved belong to the given Boolean algebra. Suppose now that X and Y are finite non-empty sets of elements in the Boolean algebra, and write

$$p = \sum X \qquad \text{and} \qquad q = \sum Y.$$

Use the preceding definitions of p and q, the equations in (1) and (2), and the associative and commutative laws for addition to arrive at

$$\begin{aligned} p\,;q = p\,;(\sum Y) &= \sum\{p\,;s : s \in Y\} = \sum\{(\sum X)\,;s : s \in Y\} \\ &= \sum\{\sum\{r\,;s : r \in X\} : s \in Y\} = \sum\{r\,;s : r \in X \text{ and } s \in Y\}. \end{aligned}$$

The proof for operations of ranks different from two is completely analogous. $\square$

A binary operation $\,;\,$ on a Boolean algebra A is said to be *monotone* if it is monotone in each argument in the sense that $s \le t$ implies

$$r\,;s \le r\,;t \qquad \text{and} \qquad s\,;r \le t\,;r$$

for all elements r, s, and t in A. A monotone operation $\,;\,$ clearly satisfies the following *general monotony law*:

$$r \le u \quad \text{and} \quad s \le v \quad \text{implies} \quad r\,;s \le u\,;v.$$

This definition and observation easily extend to operations of other ranks. Distributive operations are always monotone.

Lemma 2.3. *A distributive operation on a Boolean algebra is monotone.*

Proof. Consider the case of a distributive binary operation $\,;\,$ on a Boolean algebra. If r, s, and t are elements in the given algebra, and if $s \le t$, then $s + t = t$, by the definition of $\le$, and therefore

$$r\,;(s+t) = r\,;t \qquad \text{and} \qquad (s+t)\,;r = t\,;r.$$

Since

$$r\,;(s+t) = r\,;s + r\,;t \qquad \text{and} \qquad (s+t)\,;r = s\,;r + t\,;r,$$

it may be concluded that

$$r\,;s + r\,;t = r\,;t \qquad \text{and} \qquad s\,;r + t\,;r = t\,;r.$$

Consequently, $r\,;s \le r\,;t$ and $s\,;r \le t\,;r$, by the definition of $\le$. $\square$

Distributive laws for operations on Boolean algebras have infinitary versions as well. A binary operation $\,;\,$ on a Boolean algebra A is said to be *quasi-completely distributive*, or *quasi-complete* for short, if for all elements r in A and all non-empty subsets X of A, the existence of the sum $\sum X$ implies that the sums

$$\textstyle\sum\{r\,;s : s \in X\} \quad \text{and} \quad \sum\{s\,;r : s \in X\}$$

exist, and that

$$r\,;(\textstyle\sum X) = \sum\{r\,;s : s \in X\} \quad \text{and} \quad (\sum X)\,;r = \sum\{s\,;r : s \in X\}.$$

The operation $\,;\,$ is said to satisfy the *general quasi-complete distributivity law* if for all non-empty subsets X and Y of A, the existence of the suprema $\sum X$ and $\sum Y$ in A implies that the supremum of the set

$$\{r\,;s : r \in X \text{ and } s \in Y\}$$

exists, and (as in the case of finite subsets) that

$$(\textstyle\sum X)\,;(\textstyle\sum Y) = \textstyle\sum\{r\,;s : r \in X \text{ and } s \in Y\}.$$

If, in the preceding two definitions, the sets X and Y are allowed to be empty, then the operation $\,;\,$ is said to be *completely distributive*, or *complete* for short, and is said to satisfy the *general complete distributivity law* respectively. Warning: some authors use the term "completely distributive" to refer to what we have called "quasi-completely distributive".

The preceding definitions are easily extended to operations on A of arbitrary rank $n > 0$. Nullary operations are completely distributive by convention. As in the case of finite distributivity, unless explicitly stated otherwise, it will always be understood that the phrases "quasi-complete distributivity" and "complete distributivity" refer to distributivity over addition.

Lemma 2.4. *An operation on a Boolean algebra is quasi-completely distributive if and only if it satisfies the general quasi-complete distributivity law, and analogously for complete distributivity.*

Proof. If an operation on a Boolean algebra satisfies the general quasi-complete distributivity law, then it is certainly quasi-completely distributive (in each argument). To establish the reverse implication, consider the case of a binary operation $\,;\,$ that is quasi-completely distributive. Let X and Y be non-empty subsets of the given Boolean algebra such that the sums

$$p = \textstyle\sum X \qquad \text{and} \qquad q = \textstyle\sum Y \tag{1}$$

exist. The assumption of quasi-complete distributivity and the second equation in (1) imply that

$$p\,;q = p\,;(\textstyle\sum Y) = \textstyle\sum\{p\,;s : s \in Y\}. \tag{2}$$

In other words, the sum on the right exists and is equal to $p\,;q$. Similarly, the assumption of quasi-complete distributivity and the first equation in (1) imply that for each element s in Y,

$$p \,;s = (\textstyle\sum X) \,;s = \sum\{r \,;s : r \in X\}. \tag{3}$$

In other words, for each element s in Y, the sum on the right side exists and is equal to $p \,; s$. Combine these observations to arrive at

$$\begin{aligned} p \,;q = \textstyle\sum\{p \,;s : s \in Y\} &= \textstyle\sum\{\sum\{r \,;s : r \in X\} : s \in Y\} \\ &= \textstyle\sum\{r \,;s : r \in X \text{ and } s \in Y\}, \end{aligned}$$

by (2), (3), and the infinite associative law for addition.

A completely analogous argument applies to operations of ranks different from two. The proof that an operation is completely distributive if and only if it satisfies the general complete distributivity law can be obtained from the preceding proof by omitting everywhere the words "non-empty" and "quasi". □

It is not difficult to see that complete operations are just quasi-complete operations that are *normal* in the sense that their value on a sequence of elements is 0 whenever one of the arguments is 0. In the case of a binary operation $\,;$, this means that

$$r \,;0 = 0 \qquad \text{and} \qquad 0 \,;r = 0$$

for every element r in the algebra.

Lemma 2.5. *An operation on a Boolean algebra is complete if and only if it is quasi-complete and normal.*

Proof. Focus on the case of a binary operation $\,;$. The definitions of complete distributivity and quasi-complete distributivity for this operation differ only in one point: the set X involved in the defining equations

$$r \,;(\textstyle\sum X) = \sum\{r \,;s : s \in X\}, \qquad (\sum X) \,;r = \sum\{s \,;r : s \in X\} \tag{1}$$

is allowed to be empty in the former definition, but not in the latter. Consequently, in order to prove the lemma it suffices to show that the operation $\,;$ is normal if and only if the equations in (1) hold when the set X is empty.

Assume that X is empty, and observe that the sets

$$\{r \,;s : s \in X\} \qquad \text{and} \qquad \{s \,;r : s \in X\}$$

are then also empty, so that

$$\sum X = \sum\{r\,;s : s \in X\} = \sum\{s\,;r : s \in X\} = 0. \tag{2}$$

If $\,;\,$ is normal, then

$$r\,;(\sum X) = r\,;0 = 0 = \sum\{r\,;s : s \in X\} \qquad \text{and}$$
$$(\sum X)\,;r = 0\,;r = 0 = \sum\{s\,;r : s \in X\},$$

by (2) and the assumption that $\,;\,$ is normal, so the equations in (1) hold. On the other hand, if the equations in (1) hold, then

$$r\,;0 = r\,;(\sum X) = \sum\{r\,;s : s \in X\} = 0 \qquad \text{and}$$
$$0\,;r = (\sum X)\,;r = \sum\{s\,;r : s \in X\} = 0,$$

by (1) and (2), so the operation $\,;\,$ is normal. □

An element in a Boolean algebra is called a *quasi-atom* if it is either an atom or zero. The set of quasi-atoms in a Boolean algebra is just the set of atoms together with the zero element. A binary operation $\,;\,$ on an atomic Boolean algebra A is said to be *quasi-completely distributive for quasi-atoms*, or *quasi-complete for quasi-atoms* for short, if for any non-empty sets X and Y of quasi-atoms in A, the existence of the suprema $\sum X$ and $\sum Y$ in A implies that

$$(\sum X)\,;(\sum Y) = \sum\{r\,;s : r \in X \text{ and } s \in Y\}.$$

In other words, existence of the sums $\sum X$ and $\sum Y$ implies that the sum on the right side of the preceding equation exists and is equal to the element on the left side.

Lemma 2.6. *An operation on an atomic Boolean algebra is quasi-completely distributive if and only if it is quasi-completely distributive for quasi-atoms.*

Proof. A quasi-completely distributive operation is obviously quasi-completely distributive for quasi-atoms. To prove the reverse implication, consider the case of a binary operation $\,;\,$ on an atomic Boolean algebra A, and assume that $\,;\,$ is quasi-completely distributive for quasi-atoms. Let X and Y be non-empty subsets of A such that the suprema

$$p = \sum X \qquad \text{and} \qquad q = \sum Y$$

exist in A. It is to be shown that $p\,;q$ is the supremum of the set

$$Z = \{r\,;s : r \in X \text{ and } s \in Y\}. \tag{1}$$

For each element t in A, write A_t for the set of quasi-atoms in A that are below t. The set A_t is never empty, because it contains 0. Every element in an atomic Boolean algebra is the supremum of the set of quasi-atoms that it dominates, so t is the supremum of A_t. Observe that

$$A_p = \bigcup_{r \in X} A_r \qquad \text{and} \qquad A_q = \bigcup_{s \in Y} A_s. \tag{2}$$

For instance, if u is in A_r for some r in X, then $u \le r \le p$, and therefore u is in A_p. On the other hand, if u is in A_p, then

$$u \le p = \sum X,$$

so $u \le r$ for some r in X, because u is a quasi-atom and the set X is not empty. Therefore, u is in A_r for some r in X, by the definition of the set A_r.

Write

$$U_{rs} = \{u\,;v : u \in A_r \text{ and } v \in A_s\} \tag{3}$$

for each r in X and s in Y, and write

$$W = \{u\,;v : u \in A_p \text{ and } v \in A_q\}. \tag{4}$$

It follows from (2)–(4) that

$$W = \bigcup\{U_{rs} : r \in X \text{ and } s \in Y\}. \tag{5}$$

Use (4), the assumed quasi-complete distributivity of $;$ for quasi-atoms, and the fact that each element in A is the sum of the quasi-atoms that it dominates, to obtain

$$\begin{aligned} p\,;q &= (\textstyle\sum A_p)\,;(\textstyle\sum A_q) \\ &= \textstyle\sum\{u\,;v : u \in A_p \text{ and } v \in A_q\} = \textstyle\sum W. \end{aligned} \tag{6}$$

A similar argument, using (3) instead of (4), implies that

$$\begin{aligned} r\,;s &= (\textstyle\sum A_r)\,;(\textstyle\sum A_s) \\ &= \textstyle\sum\{u\,;v : u \in A_r \text{ and } v \in A_s\} = \textstyle\sum U_{rs} \end{aligned} \tag{7}$$

for each r in X and s in Y.

Since $\sum W$ exists, by (6), and $\sum U_{rs}$ exists for each r in X and s in Y, by (7), it follows from (5) and the infinite associative law for addition that

$$\sum W = \sum\{\sum U_{rs} : r \in X \text{ and } s \in Y\}. \tag{8}$$

In other words, the sum on the right exists and is equal to the sum on the left. Combine (6), (7), and (8) with (1) to arrive at the desired conclusion:

$$\begin{aligned} p \,;q = \sum W = \sum\{\sum U_{rs} : r \in X \text{ and } s \in Y\} \\ = \sum\{r \,; s : r \in X \text{ and } s \in Y\} = \sum Z. \end{aligned}$$

The argument for operations of any finite non-zero rank is entirely analogous. □

A binary operation ; on an atomic Boolean algebra A is said to be *completely distributive for atoms*, or *complete for atoms* for short, if for any sets X and Y of atoms in A, the existence of the suprema $\sum X$ and $\sum Y$ in A implies that

$$(\sum X) \,; (\sum Y) = \sum\{r \,; s : r \in X \text{ and } s \in Y\}.$$

In other words, existence of the sums $\sum X$ and $\sum Y$ implies that the sum on the right side of the preceding equation exists and is equal to the element on the left side. Notice that the sets X and Y are allowed to be empty.

Lemma 2.7. *An operation on an atomic Boolean algebra is completely distributive if and only if it is completely distributive for atoms.*

Proof. One approach to proving the lemma is to imitate the proof of Lemma 2.6, deleting the term "quasi-" everywhere, and allowing the sets X and Y to be empty. Another approach is to derive the lemma directly from Lemma 2.6. We take the latter approach.

A completely distributive operation is obviously completely distributive for atoms. To prove the reverse implication, consider the case of a binary operation ; on an atomic Boolean algebra A, and assume that ; is completely distributive for atoms. Notice that ; must be a normal operation. For example, for any element p in A, take X to be the set of atoms below p, and Y to be the empty set. Clearly,

$$p = \sum X \qquad \text{and} \qquad 0 = \sum Y, \tag{1}$$

by the assumption that A is atomic. Consequently,

$$p\,;0 = (\sum X)\,;(\sum Y) = \sum\{r\,;s : r \in X \text{ and } s \in Y\} = \sum\varnothing = 0,$$

by (1), the assumed complete distributivity of the operation $;$ for atoms, and the assumption that the set Y is empty. An analogous argument shows that $0\,;r = 0$.

To prove that $;$ is quasi-completely distributive for quasi-atoms, consider non-empty sets X and Y of quasi-atoms in A such that the suprema

$$p = \sum X \qquad \text{and} \qquad q = \sum Y \tag{2}$$

exist in A. It is to be shown that $p\,;q$ is the supremum of the set

$$Z = \{r\,;s : r \in X \text{ and } s \in Y\}. \tag{3}$$

Take X_0 and Y_0 be the sets of atoms in X and Y respectively, and put

$$Z_0 = \{r\,;s : r \in X_0 \text{ and } s \in Y_0\}. \tag{4}$$

The sets X_0 and Y_0 differ from X and Y only in that they cannot contain 0 and may therefore be empty. Clearly,

$$p = \sum X_0 \qquad \text{and} \qquad q = \sum Y_0, \tag{5}$$

by (2). The assumption that the operation $;$ is completely distributive for atoms implies that

$$p\,;q = \sum Z_0, \tag{6}$$

by (4) and (5).

If 0 does not belong to either of the sets X and Y, then

$$X = X_0, \qquad Y = Y_0, \qquad \text{and} \qquad Z = Z_0,$$

by (3) and (4). If 0 does belong to at least one of the sets X and Y, then 0 belongs to the set Z, by (3), because the operation $;$ is normal; and therefore $Z = Z_0 \cup \{0\}$. In either case, $\sum Z = \sum Z_0$, so

$$p\,;q = \sum Z_0 = \sum Z,$$

by (6). Consequently, $;$ is quasi-completely distributive for quasi-atoms, as claimed.

Apply Lemma 2.6 to conclude that $;$ is quasi-completely distributive. Since $;$ is also normal, it follows by Lemma 2.5 that $;$ is completely distributive. The argument for operations of any finite non-zero rank is entirely analogous. □

An operation on a Boolean algebra that is distributive (in each argument) is traditionally called an *operator*. Distinguished constants are vacuously seen to be operators. A Boolean algebra that has been expanded by adjoining to it a system of operators as fundamental operations is called a *Boolean algebra with operators*. If each of the operators of rank at least one is normal, then one speaks of a *Boolean algebra with normal operators*. Similarly, if each of the operators of rank at least one is quasi-complete, or complete, then one speaks of a *Boolean algebra with quasi-complete operators*, or *complete operators*, respectively.

In order to keep the notation as simple as possible when considering Boolean algebras with operators, we shall restrict our attention to algebras of the form

$$\mathfrak{A} = (A\,, +\,, -\,, ;\,, {}^{\smile}\,, 1'),$$

where $+$ and $;$ are binary operations, while $-$ and ${}^{\smile}$ are unary operations, and 1' is a distinguished constant. Such algebras are said to be *similar* to, or of the *same similarity type* as, relation algebras. When speaking of a Boolean algebra with operators, *we shall always assume that the algebra in question has the preceding form*, so for us, a Boolean algebra with operators is an algebra $\mathfrak{A}$ of the same similarity type as a relation algebra, in which Axioms (R1)–(R3), (R8), the dual of (R8), and (R9) hold in $\mathfrak{A}$. It is very important to note, however, that all definitions and results given in this work for such Boolean algebras with operators can, with minor and obvious modifications in the statements and proofs, be extended to Boolean algebras with operators of an arbitrary similarity type.

In referring to the operations and distinguished constants of a relation algebra (or a Boolean algebra with operators), we shall usually use the same symbol to refer to the corresponding operations or distinguished constants of different algebras. For instance, we shall usually use the symbol $+$ to refer to the operation of addition in relation algebras $\mathfrak{A}$ and $\mathfrak{B}$, even when speaking about both algebras at the same time. Similarly, we shall usually use the symbol 1' to refer to the identity element in $\mathfrak{A}$ and in $\mathfrak{B}$, even when speaking about both algebras at the same time. This convention is very common in mathematical practice; it simplifies the notation, renders the notation easier to read, and usually does not lead to confusion because the context makes clear whether the symbol being used is referring to an operation (or distinguished constant) in $\mathfrak{A}$ or in $\mathfrak{B}$. (For a concrete example

from ordinary mathematics, the symbol $+$ is used to denote addition of natural numbers, of rational numbers, of real numbers, of complex numbers, of elements in an arbitrary abelian group, and of elements in an arbitrary Boolean algebra.) In ambiguous cases, it is possible to clarify the intended use of the symbol explicitly, either in words or with the help of some sort of symbolism. For example, we could use notation such as $+^{\mathfrak{A}}$ and $+^{\mathfrak{B}}$ to distinguish the operations of addition in $\mathfrak{A}$ and in $\mathfrak{B}$.

2.3 Verifying axioms

The process of verifying that a given algebra satisfies the axioms of relation algebra is often a rather tedious task. If the given algebra is constructed from a Boolean algebra—for example, from a Boolean algebra of subsets of a given set—and if that Boolean algebra is atomic, then the process can usually be streamlined. It may only be necessary to check the validity of a few of the relation algebraic axioms, and then only with respect to the atoms of the algebra. The next theorem gives an example of this phenomenon.

Theorem 2.8. *Suppose* $(A\,,+\,,-)$ *is an atomic Boolean algebra. If* $\,;\,$ *and* $^\smile$ *are, respectively, binary and unary operations on* A *that are completely distributive for atoms, and if* $1'$ *is an element in* A, *then*

$$\mathfrak{A} = (A\,,+\,,-\,,;\,,{}^\smile\,,1')$$

is a relation algebra if and only if (R4)–(R7) *and* (R11) *hold for all atoms* r, s, *and* t *in* $\mathfrak{A}$.

Proof. The implication from left to right is trivially true. To establish the reverse implication, it must be shown that that if (R4)–(R7) and (R11) are true for all atoms in $\mathfrak{A}$, then they are true for all elements in $\mathfrak{A}$. Notice that (R1)–(R3) hold by assumption, and (R8) and (R9) hold by Lemma 2.7 and the assumption that $;$ and $^\smile$ are completely distributive for atoms.

As an example, here is the verification of (R11). Assume (R11) holds for atoms, and consider arbitrary elements r, s, and t in $\mathfrak{A}$. It is to be shown that (R11) holds for r, s, and t. Let U, V, and W be the sets of atoms in $\mathfrak{A}$ that are below these elements respectively. Every element

in an atomic Boolean algebra is the supremum of the set of atoms that it dominates, so

$$r = \sum U, \qquad s = \sum V, \qquad t = \sum W, \tag{1}$$

and therefore

$$(r\,;s)\cdot t = [(\sum U)\,;(\sum V)]\cdot(\sum W) \tag{2}$$

and

$$(r^{\smile}\,;t)\cdot s = [(\sum U)^{\smile}\,;(\sum W)]\cdot(\sum V). \tag{3}$$

The operations ; and $^{\smile}$ are assumed to be completely distributive for atoms, so they are completely distributive, by Lemma 2.7; and the Boolean operation of multiplication is also completely distributive. The sets

$$X = \{(u\,;v)\cdot w : u \in U, v \in V, w \in W\} \tag{4}$$

and

$$Y = \{(u^{\smile}\,;w)\cdot v : u \in U, v \in V, w \in W\} \tag{5}$$

therefore have suprema in $\mathfrak{A}$, and in fact

$$\sum X = [(\sum U)\,;(\sum V)]\cdot(\sum W) \tag{6}$$

and

$$\sum Y = [(\sum U)^{\smile}\,;(\sum W)]\cdot(\sum V), \tag{7}$$

by (1).

The hypothesis of (R11) is that $(r\,;s)\cdot t = 0$. From this equation, together with (2) and (6), it follows that $\sum X = 0$. Consequently,

$$(u\,;v)\cdot w = 0$$

for all elements u, v, and w in U, V, and W respectively, by (4) and Boolean algebra. Apply (R11) for atoms to obtain

$$(u^{\smile}\,;w)\cdot v = 0$$

for all u, v and w in U, V, and W respectively. Therefore, $\sum Y = 0$, by (5). Combine this equation with (7) to arrive at

$$[(\sum U)^{\smile} ; (\sum W)] \cdot (\sum V) = 0.$$

In view of (3), it may be concluded that $(r^{\smile} ; t) \cdot s = 0$, as desired.

The verification of (R4)–(R7) can be handled in an entirely analogous fashion. The details are left as an exercise. □

There are several key points that allow the preceding proof to go through. First, the only operations that occur in (R4)–(R7) and (R11) are operations that are completely distributive. In particular, the operation of complement does not occur in these axioms. Second, each of these axioms has the form of an equation or of an implication between equations. Third, in each equation a given variable occurs at most once on each side of the equation. Finally, it is necessary to assume complete distributivity for atoms instead of quasi-complete distributivity for atoms because it is necessary to take into account the cases when one or more of the elements r, s, and t are zero.

Theorem 2.8 is quite useful, but it has a drawback: the verification of (R4), (R5), and (R7) for atoms may involve computations of relative products and converses of elements that are not atoms. For example, in order to verify (R4) for atoms r, s, and t, one must first compute the relative products $r ; s$ and $s ; t$. Neither of these relative products need be an atom, so in computing $(r ; s) ; t$ and $r ; (s ; t)$, one is computing relative products of atoms with elements that may not be atoms. It is sometimes more advantageous to use a form of Theorem 2.8 that involves computations of relative products and converses for atoms only.

Theorem 2.9. *Suppose* $(A\,,+\,,-)$ *is an atomic Boolean algebra. If* $;$ *and* $^{\smile}$ *are, respectively, binary and unary operations on* A *that are completely distributive for atoms, and if* 1' *is an element in* A, *then*

$$\mathfrak{A} = (A\,,+\,,-\,,;\,,{}^{\smile}\,,1')$$

is a relation algebra if and only if the converse of every atom is an atom, and the following conditions hold for all atoms p, r, s, *and* t *in* $\mathfrak{A}$.

(i) *If* $p \leq r ; q$ *for some atom* $q \leq s ; t$ *then* $p \leq q ; t$ *for some atom* $q \leq r ; s$.

(ii) $r \,;s = 0$ *or* $r \,;s = r$ *whenever* s *is an atom below* 1', *and* $r \,;s = r$ *for at least one such atom* s.
(iii) *If* $t \le r \,;s$, *then* $t^{\smile} \le s^{\smile} \,;r^{\smile}$.
(iv) *If* $t \le r \,;s$, *then* $s \le r^{\smile} \,;t$.

Proof. We begin with two preliminary observations. First, under the hypothesis that $\mathfrak{A}$ is an atomic relation algebra, the operation of converse in $\mathfrak{A}$ must map the set of atoms bijectively to itself (see Lemma 4.1(vii)) and Axiom (R6) must hold for all atoms, that is to say,

$$r^{\smile\smile} = r \tag{1}$$

for every atom r in $\mathfrak{A}$. Second, under the hypothesis that $\mathfrak{A}$ is an algebra satisfying the conditions of the theorem, the operation $^{\smile}$ must map the set of atoms bijectively to itself, and (1) must hold for all atoms. To prove this second observation, fix an atom r in $\mathfrak{A}$, and notice that $r^{\smile}$ and $r^{\smile\smile}$ are also atoms, by the assumption that $^{\smile}$ maps atoms to atoms. There is an atom s below 1' such that $r = r \,;s$, by the second part of (ii). Apply condition (iv) twice, first with r in place of t to obtain $s \le r^{\smile} \,;r$, and then with $r^{\smile}$, r, and s in place of r, s, and t respectively to obtain $r \le r^{\smile\smile} \,;s$. The product $r^{\smile\smile} \,;s$ is either 0 or $r^{\smile\smile}$, by the first part of condition (ii), and it cannot be 0, because the product is above the atom r. Consequently, $r^{\smile\smile} \,;s = r^{\smile\smile}$ and therefore $r \le r^{\smile\smile}$. The validity of (1) for r follows at once from this last inequality and the fact that r and $r^{\smile\smile}$ are atoms.

The validity of (1) for atoms easily implies that the operation $^{\smile}$ maps the set of atoms bijectively to itself. Indeed, if r and s are atoms such that $r^{\smile} = s^{\smile}$, then $r^{\smile\smile} = s^{\smile\smile}$, and therefore $r = s$, by (1). Also, every atom r is the image under $^{\smile}$ of an atom, namely the atom $r^{\smile}$.

On the basis of the observations of the preceding paragraphs—namely that under either hypothesis, the operation $^{\smile}$ maps the set of atoms bijectively to itself, and (1) holds for atoms—we shall show that conditions (ii), (iii), and (iv) are respectively equivalent to the validity of (R5), (R7), and (R11) for atoms, and on the basis of (iii) and (1), condition (i) is equivalent to the validity of (R4) for atoms. The theorem then follows from Theorem 2.8. In the arguments below, the variables p, q, r, s, and t range over the set of atoms in $\mathfrak{A}$.

If condition (iv) holds for all atoms r, s, and t, then by replacing r with $r^{\smile}$ and interchanging s and t in (iv), and applying (1), we arrive at the implication

$$s \leq r^{\smile} \,;\, t \qquad \text{implies} \qquad t \leq r \,;\, s,$$

which is just the contrapositive of (R11) for atoms. On the other hand, if (R11) holds for all atoms, then by replacing r with $r^{\smile}$ and interchanging s and t in (R11), and applying (1), we arrive at the contrapositive of condition (iv), namely

$$(r^{\smile} \,;\, t) \cdot s = 0 \qquad \text{implies} \qquad (r \,;\, s) \cdot t = 0.$$

Thus, condition (iv) is equivalent to the validity of (R11) for atoms.

Turn next to the proof that condition (iii) is equivalent to the validity of (R7) for atoms. Assume first that condition (iii) holds for all atoms r, s, and t. Take atoms $s^{\smile}$, $r^{\smile}$, and $t^{\smile}$ for r, s, and t respectively in condition (iii), and then invoke (1), to obtain

$$t^{\smile} \leq s^{\smile} \,;\, r^{\smile} \qquad \text{implies} \qquad t \leq r \,;\, s.$$

This implication, together with condition (iii) and the fact that $^{\smile}$ is a bijection of the set of atoms, shows that $^{\smile}$ maps the set of atoms below $r \,;\, s$ bijectively to the set of atoms below $s^{\smile} \,;\, r^{\smile}$. Consequently,

$$\{t^{\smile} : t \leq r \,;\, s\} = \{q : q \leq s^{\smile} \,;\, r^{\smile}\}. \tag{2}$$

Since $\mathfrak{A}$ is atomic, every element is the sum of the atoms it dominates. In particular,

$$r \,;\, s = \sum\{t : t \leq r \,;\, s\} \qquad \text{and} \qquad s^{\smile} \,;\, r^{\smile} = \sum\{q : q \leq s^{\smile} \,;\, r^{\smile}\}. \tag{3}$$

The operation $^{\smile}$ is assumed to be completely distributive for atoms, so the supremum of the set $\{t^{\smile} : t \leq r \,;\, s\}$ exists, and in fact

$$\sum\{t^{\smile} : t \leq r \,;\, s\} = (\sum\{t : t \leq r \,;\, s\})^{\smile} = (r \,;\, s)^{\smile}, \tag{4}$$

by the first equation in (3). Combine (4) with (2) and the second equation in (3) to arrive at

$$(r \,;\, s)^{\smile} = s^{\smile} \,;\, r^{\smile}. \tag{5}$$

Thus, (R7) holds for atoms.

To prove the reverse implication, assume (R7) holds for all atoms. In particular, (5) holds for two given atoms r and s. The hypothesis that the operation $^{\smile}$ is completely distributive for atoms implies that it is completely distributive, by Lemma 2.7, and therefore monotone, by Lemma 2.3. Consider now an arbitrary atom t in $\mathfrak{A}$. If $t \leq r \,;\, s$,

then $t^{\smile} \leq (r\,;s)^{\smile}$, by the monotony of $^{\smile}$, and therefore $t^{\smile} \leq s^{\smile}\,;r^{\smile}$, by (5). Thus, condition (iii) holds.

The remaining two arguments are similar in spirit to the preceding ones, so we shall be briefer in our presentation. Consider first the equivalence of condition (i) with (R4) for atoms. On the basis of (1) and condition (iii), condition (i) implies its own converse. Indeed, suppose condition (i) holds for all atoms p, r, s, and t. To establish the converse, assume that

$$p \leq q\,;t \qquad \text{for some} \qquad q \leq r\,;s. \tag{7}$$

As was shown in the preceding paragraphs, on the basis of (1), condition (iii) implies (R7) for atoms. Therefore, by applying the operation $^{\smile}$ to both inequalities in (7), and using the monotony of $^{\smile}$, together with (R7) for atoms, we obtain

$$p^{\smile} \leq t^{\smile}\,;q^{\smile} \qquad \text{for some} \qquad q^{\smile} \leq s^{\smile}\,;r^{\smile}. \tag{8}$$

If the atoms p, q, r, s, and t in condition (i) are respectively replaced by the atoms $p^{\smile}$, $q^{\smile}$, $t^{\smile}$, $s^{\smile}$, and $r^{\smile}$, then the hypothesis of condition (i) assumes the form of (8), and the conclusion of the condition assumes the form

$$p^{\smile} \leq q^{\smile}\,;r^{\smile} \qquad \text{for some} \qquad q^{\smile} \leq t^{\smile}\,;s^{\smile}. \tag{9}$$

Apply $^{\smile}$ to the inequalities in (9), and use the monotony of $^{\smile}$, (R7) for atoms, and (1) to conclude that

$$p \leq r\,;q \qquad \text{for some} \qquad q \leq s\,;t. \tag{10}$$

Thus, the hypothesis (7) implies the conclusion (10), which is just what the converse of condition (i) says.

The equality

$$r\,;(s\,;t) = (r\,;s)\,;t \tag{11}$$

holds for atoms r, s, and t just in case every atom p below the left side is also below the right side, and vice versa. The complete distributivity of the operation $;$ for atoms implies that p will be below the left side just in case there is an atom q below $s\,;t$ such that $p \leq r\,;q$. Similarly, p will be below the right side just in case there is an atom $q \leq r\,;s$ such that $p \leq q\,;t$. Consequently, equation (11) holds atoms just in

case condition (i) and its converse hold. Since condition (i) implies its converse, by the observations of the preceding paragraph, it follows that condition (i) is equivalent to the validity of (R4) for atoms.

It remains to treat condition (ii). The element 1' is the sum of the atoms in $\mathfrak{A}$ that it dominates, so

$$r\,;1' \leq r \qquad \text{if and only if} \qquad r\,;s \leq r \tag{12}$$

for every atom $s \leq 1'$, by the complete distributivity of the operation ; for atoms. Since r is an atom, the inequality on the right side of (12) is equivalent to saying that $r\,;s = 0$ or $r\,;s = r$ for every atom $s \leq 1'$. Consequently, the equality $r\,;1' = r$ is equivalent to the validity of the inequality on the right side of (12) for all atoms $s \leq 1'$, together with the requirement that $r\,;s = r$ for some atom $s \leq 1'$. □

The preceding proof establishes more than is claimed in the statement of the theorem. It shows that if (R6) is valid in an atomic Boolean algebra with completely distributive operators $\mathfrak{A}$, then (R5) is valid in $\mathfrak{A}$ if and only if condition (ii) of the theorem holds for all atoms, (R7) is valid in $\mathfrak{A}$ if and only if condition (iii) holds for all atoms, and (R11) is valid in $\mathfrak{A}$ if and only if condition (iv) holds for all atoms. It also shows that if (R6) and (R7) are valid in $\mathfrak{A}$, then (R4) is valid in $\mathfrak{A}$ if and only if condition (i) holds for all atoms. Since (R10) is equivalent to (R11) in any Boolean algebra with operators in which (R6) and (R7) are valid (see the relevant remarks at the end of Section 2.1), it follows that if (R6) and (R7) are valid in $\mathfrak{A}$, then (R10) is valid in $\mathfrak{A}$ if and only if condition (iv) holds for all atoms. These consequences are particularly helpful when verifying that some, but not necessarily all, of (R4)–(R7) and (R10) hold in a Boolean algebra with completely distributive operators.

2.4 Language of relation algebras

For the most part, the development of the theory of relation algebras can proceed in an informal fashion, without any reference to logic—just as is the case with most algebraic theories such as group theory and ring theory. At times, however, notions and methods of first-order logic do play an important role. The purpose of this section is to provide a brief introduction to the relevant logical notions and notation that we shall need.

The *first-order language of relation algebras*—also called the *elementary language of relation algebras*—is a language $\mathcal{L}$ with two types of symbols, logical and non-logical. The logical symbols of $\mathcal{L}$ include a countably infinite sequence of variables

$$v_0, v_1, v_2, \ldots, v_n, \ldots,$$

and we occasionally write $\boldsymbol{x}$, $\boldsymbol{y}$, and $\boldsymbol{z}$ for the first three of these variables. There is also a binary relation symbol $=$ denoting the relation of equality between individuals. In addition, there are two sentential connectives, namely a symbol $\neg$ for *negation* and a symbol $\rightarrow$ for *implication*, there is a symbol $\forall$ for *universal quantification*, and there are parentheses (and).

The non-logical symbols of $\mathcal{L}$ consist of an individual constant symbol 1', two binary operation symbols $+$ and $;$, and two unary operation symbols $-$ and $\smile$. Formally speaking, we should use some notational device to distinguish between the operation symbols of $\mathcal{L}$ and the operations of a relation algebra $\mathfrak{A}$, for example by writing the former in boldface and the latter in lightface, or by writing both in lightface but adding a superscript $\mathfrak{A}$ to the latter, as in $+^{\mathfrak{A}}$. In practice, there is usually little danger of confusion, so the cumbersome additional notation may for the most part be omitted. We employ it only when it seems necessary.

An *expression* is any string of symbols in $\mathcal{L}$. Terms and formulas are special kinds of expressions. Terms are built up from variables and the individual constant symbol by an inductive process using the operation symbols: variables and the individual constant symbol 1' are *atomic terms* (this is the *base case*, or *base clause*, of the definition); if σ and τ are terms, then so are

$$(\sigma + \tau), \qquad (-\sigma), \qquad (\sigma \,;\, \tau), \qquad \text{and} \qquad (\sigma^{\smile})$$

(this is the *induction case*, or the *induction clause*, of the definition); and an expression is a *term* if and only if it can be shown to be a term by a finite number of applications of the base clause and the induction clause. In order to simplify notation, we follow the standard conventions regarding the way in which terms are to be read when parentheses are omitted: unary operation symbols take precedence over binary operation symbols, and among binary operation symbols, multiplication symbols take precedence over addition symbols (and outer parentheses are always omitted). For example,

$$v_0^{\smile} + -v_1 \,;\, v_2^{\smile} \qquad \text{abbreviates} \qquad ((v_0^{\smile}) + ((-v_1) \,;\, (v_2^{\smile})))$$

The notation $\sigma(v_0, \ldots, v_{n-1})$ indicates that σ is a term and the variables occurring in σ form a subset of $\{v_0, \ldots, v_{n-1}\}$.

The inductive definition of a term carries with it a method for proving that all terms possess a given property: one shows first that all variables and the individual constant symbol 1' possess the property (this is called the *base case* of the proof), and then one shows that if terms σ and τ possess the property, then so do the terms obtained from σ and τ by the induction clause of the definition (this is called the *induction step* of the proof). This method of proof is called *proof by induction on terms.* The definition of a term also carries with it an analogous method for defining notions that apply to terms; such a definition is called a *definition by induction on terms.*

Formulas are also defined by an inductive process, using sentential connectives and quantifiers. *Atomic formulas* are *equations* $\sigma = \tau$, where σ and τ are terms (this is the *base case*, or *base clause*, of the definition); if Γ and Δ are formulas, then so are

$$(\Gamma \rightarrow \Delta), \qquad (\neg\Gamma), \qquad \text{and} \qquad (\forall v \Gamma)$$

for every variable v (this is the *induction case*, or the *induction clause*, of the definition); and an expression is a *formula* if and only if it can be shown to be a formula by a finite number of applications of the base clause and the induction clause. The symbols $\vee$, $\wedge$, $\leftrightarrow$, and $\exists$ for *disjunction*, *conjunction*, *equivalence* (or *bi-implication*), and *existential quantification* respectively, are introduced as abbreviations in the usual manner:

$$\begin{array}{lll}
(\Gamma \vee \Delta) & \text{abbreviates} & ((\neg\Gamma) \rightarrow \Delta), \\
(\Gamma \wedge \Delta) & \text{abbreviates} & (\neg(\Gamma \rightarrow (\neg\Delta))), \\
(\Gamma \leftrightarrow \Delta) & \text{abbreviates} & (\neg((\Gamma \rightarrow \Delta) \rightarrow (\neg(\Delta \rightarrow \Gamma)))), \\
(\exists v_i \Gamma) & \text{abbreviates} & (\neg(\forall v_i(\neg\Gamma))).
\end{array}$$

We follow the standard conventions regarding the omission of parentheses when writing formulas: $\neg$ has priority over $\vee$ and $\wedge$, which in turn have priority over $\rightarrow$ and $\leftrightarrow$ (and outer parentheses are always omitted). For example, the formula

$$\Gamma_0 \wedge \cdots \wedge \Gamma_{n-1} \rightarrow \Gamma_n$$

is to be understood as follows: the conjunction of formulas $\Gamma_0, \dots, \Gamma_{n-1}$ implies the formula Γ_n.

Just as with the definition of a term, the inductive definition of a formula carries with it a method for proving that all formulas possess a given property: one shows first that all atomic formulas possess the property (this is the *base case* of the proof), and then one shows that if formulas Γ and Δ possess the property, then so do the formulas obtained from Γ and Δ by the induction clause of the definition (this is the *induction step* of the proof). This method of proof is called *proof by induction on formulas.* The definition of a formula also carries with it an analogous method for defining notions that apply to formulas; such a definition is called a *definition by induction on formulas.*

Here is an example: the definition of the notion of a variable occurring free in a formula proceeds by induction on formulas. Base clause: a variable v_i *occurs free* in an atomic formula Γ if v_i is one of the symbols in Γ. Induction clause: the variable v_i occurs free in $\neg\Gamma$ if it occurs free in Γ, it occurs free in $\Gamma \rightarrow \Delta$ if it occurs free in Γ or in Δ, and it occurs free in $\exists v_j \Gamma$ if it occurs free in Γ and is not equal to v_j. Warning: a variable v_i may occur free in a formula Γ, and still be *bound* in some subformula of Γ in the sense that v_i occurs in the subformula but is not free in that subformula. The notation $\Gamma(v_0, \dots, v_{n-1})$ indicates that Γ is a formula and the variables occurring free in Γ form a subset of $\{v_0, \dots, v_{n-1}\}$.

Various special kinds of formulas are of particular importance in the study of relation algebras. Here are some examples. A *sentence* is a formula in which no variables occur free. A *quantifier-free formula*, or an *open formula*, is a formula in which no quantifiers occur at all. A *universal formula* is a formula of the form $\forall v_{i_0} \dots \forall v_{i_{n-1}} \Delta$, where Δ is a quantifier-free formula, and an *existential formula* is defined analogously, with $\forall$ replaced by $\exists$; if the formula is in fact a sentence, then we speak of a *universal sentence* or an *existential sentence* respectively. A *positive formula* is a formula built up from equations using only conjunction, disjunction, and existential and universal quantification, and a *positive sentence* is a positive formula that is also a sentence. A *conditional equation* is a quantifier-free formula of the form

$$(\varepsilon_0 \wedge \varepsilon_1 \wedge \cdots \wedge \varepsilon_{n-1}) \rightarrow \varepsilon_n,$$

where $\varepsilon_0, \varepsilon_1, \dots, \varepsilon_n$ are equations. A *universal Horn formula* is a universal formula in which the quantifier-free part Δ is either a disjunction of negations of equations or else a conditional equation; equivalently, Δ

is a disjunction consisting of negations of equations and at most one unnegated equation; if the formula is in fact a sentence, then we speak of a *universal Horn sentence*, and if it is quantifier-free, then we speak of a (*basic*, or *open*) *Horn formula.* An *identity* is a universal sentence in which the quantifier-free part is a single equation.

Associated with the language of relation algebras are a series of semantic notions that we shall need. Fix an algebra

$$\mathfrak{A} = (A\,,+\,,-\,,;\,,\,^{\smile}\,,1’\,)$$

of the same similarity type as relation algebras, and write A^n for the set of sequences of the form

$$r = (r_0, \ldots, r_{n-1}),$$

where $r_0, \ldots, r_{n-1}$ are all in $\mathfrak{A}$.

Every term $\gamma(v_0, \ldots, v_{n-1})$ (whose variables are, by convention, among $v_0, \ldots, v_{n-1}$) determines an operation of rank n on the universe of $\mathfrak{A}$. This operation is called the *polynomial* (*of rank* n) *induced by* γ, and it is denoted by $\gamma^{\mathfrak{A}}$. It is defined by induction on terms. The base clause of the definition concerns variables and constants. If γ is a variable v_i (for some $i < n$), then $\gamma^{\mathfrak{A}}$ is the ith *projection* (*of rank* n), that is to say, it is the operation of rank n that maps each sequence r in A^n to its ith coordinate r_i. If γ is the constant symbol 1’, then $\gamma^{\mathfrak{A}}$ is the constant operation of rank n that maps each sequence r in A^n to the distinguished constant 1’ in $\mathfrak{A}$. For the induction clause of the definition, suppose that γ has one of the forms

$$\sigma + \tau, \qquad -\sigma, \qquad \sigma\,;\tau, \qquad \sigma^{\smile},$$

where σ and τ are terms for which the polynomials $\sigma^{\mathfrak{A}}$ and $\tau^{\mathfrak{A}}$ of rank n have already been defined. The polynomial $\gamma^{\mathfrak{A}}$ is defined by specifying that for each sequence r in A^n, the value of $\gamma^{\mathfrak{A}}(r)$ is

$$\sigma^{\mathfrak{A}}(r) + \tau^{\mathfrak{A}}(r), \qquad -\sigma^{\mathfrak{A}}(r), \qquad \sigma^{\mathfrak{A}}(r)\,;\tau^{\mathfrak{A}}(r), \qquad \sigma^{\mathfrak{A}}(r)^{\smile}$$

respectively. (The first occurrences of $+$, $-$, $;$, and $^{\smile}$ above refer to symbols in $\mathcal{L}$, while the second occurrences refer to the corresponding operations in $\mathfrak{A}$.) When the context makes clear which algebra $\mathfrak{A}$ is intended, we shall usually omit the superscript and write simply $\gamma(r_0, \ldots, r_{n-1})$ or $\gamma(r)$ for the value of $\gamma^{\mathfrak{A}}$ on r, and we shall even refer to $\gamma(r)$ as the value of the *term* γ on r.

There is an ambiguous point in the preceding definition that should be clarified. A term γ with variables among $v_0, \ldots, v_{m-1}$ also has variables among $v_0, \ldots, v_{n-1}$ for each natural number $n \geq m$, and therefore γ induces a polynomial of rank n in $\mathfrak{A}$ for each such n. For example, the term $v_0 + v_2$ induces a polynomial of rank 3 in $\mathfrak{A}$ that maps each triple (r_0, r_1, r_2) to the sum $r_0 + r_2$, and it also induces a polynomial of rank 4 that maps each quadruple (r_0, r_1, r_2, r_3) to the sum $r_0 + r_2$. The notation $\gamma(v_0, \ldots, v_{n-1})$ is used to indicate that the intended polynomial induced by γ is the one of rank n.

The notion of a sequence of elements satisfying a formula in $\mathfrak{A}$ is defined by induction on formulas. Let $\varGamma$ be a formula whose free and bound variables are among $v_0, \ldots, v_{n-1}$, and let r be a sequence of n elements in $\mathfrak{A}$. The base clause of the definition says that if $\varGamma$ is an equation of the form $\sigma = \tau$, then r *satisfies* $\varGamma$ in $\mathfrak{A}$ just in case the values of σ and τ on r—that is to say, the elements $\sigma(r)$ and $\tau(r)$ in $\mathfrak{A}$—are the same. The induction clause splits into three cases: if $\varGamma$ is the formula $\neg\varDelta$, then r satisfies $\varGamma$ (in $\mathfrak{A}$) just in case r does not satisfy $\varDelta$; if $\varGamma$ is the formula $\varDelta \rightarrow \varOmega$, then r satisfies $\varGamma$ just in case r satisfies $\varOmega$ whenever it satisfies $\varDelta$; and if $\varGamma$ is the formula $\forall v_i \varDelta$, then r satisfies $\varGamma$ just in case every sequence s obtained from r by replacing r_i with an arbitrary element in $\mathfrak{A}$ satisfies the formula $\varDelta$. It is easy to check that r satisfies a disjunction $\varDelta \vee \varOmega$ just in case r satisfies at least one of $\varDelta$ and $\varOmega$, and r satisfies a conjunction $\varDelta \wedge \varOmega$ just in case r satisfies both $\varDelta$ and $\varOmega$. Also, r satisfies the formula $\exists v_i \varDelta$ just in case there is a sequence s obtained from r by replacing r_i with some element in $\mathfrak{A}$ such that s satisfies $\varDelta$. Notice that only the free variables occurring in $\varGamma$ really matter in the definition of satisfaction. In other words, if r and t are two n-termed sequences of elements in $\mathfrak{A}$ such that $r_i = t_i$ whenever v_i occurs free in $\varGamma$, then either r and t both satisfy $\varGamma$, or neither of them satisfies $\varGamma$. For that reason, we shall usually not bother to refer to the bound variables of $\varGamma$ in the future.

The semantical notions of truth and model are defined in terms of satisfaction. A formula $\varGamma$ with free variables among $v_0, \ldots, v_{n-1}$ is *true* in $\mathfrak{A}$ if it is satisfied by every n-termed sequence $(r_0, \ldots, r_{n-1})$ of elements in $\mathfrak{A}$, and $\varGamma$ *fails* in $\mathfrak{A}$ if there is some n-termed sequence of elements in $\mathfrak{A}$ that does not satisfy $\varGamma$. If $\varGamma$ is true in $\mathfrak{A}$, then $\mathfrak{A}$ is called a *model of* $\varGamma$. These notions are extended from formulas to sets of formulas, and from individual algebras to classes of algebras, in the obvious way: a set of formulas $\mathcal{S}$ is true in $\mathfrak{A}$ if every formula in $\mathcal{S}$ is true in $\mathfrak{A}$, and in this case $\mathfrak{A}$ is called a *model* of $\mathcal{S}$. More generally, $\mathcal{S}$

is true in a class of algebras K if $\mathcal{S}$ is true in every algebra in K. The class of all models of a set of formulas $\mathcal{S}$ is denoted by $\mathsf{Mo}(\mathcal{S})$.

The language $\mathcal{L}$ is also provided with a deductive apparatus: a set of logical axioms and a set of finitary rules of inference (such as modus ponens and the rule of substitution). The precise nature of this deductive apparatus is not important for our development. What does matter is that it is strong enough to prove the *Completeness Theorem* for first-order logic, which says that a formula Γ is derivable from a set of formulas $\mathcal{S}$ with the help of the logical axioms and rules of inference of $\mathcal{L}$ if and only if every algebra $\mathfrak{A}$ that is a model of $\mathcal{S}$ is also a model of Γ. A consequence of the Completeness Theorem is the *Compactness Theorem*. It says that a set of formulas $\mathcal{S}$ in $\mathcal{L}$ has a model whenever every finite subset of $\mathcal{S}$ has a model.

A set of formulas $\mathcal{T}$ in $\mathcal{L}$ is called a *first-order theory*, or an *elementary theory*, if it is closed under the *relation of provability*, that is to say, if a formula Γ is provable from a set of formulas in $\mathcal{T}$ using the deductive apparatus of $\mathcal{L}$, then Γ belongs to $\mathcal{T}$. An *axiomatization*, or a *set of axioms*, of a theory $\mathcal{T}$ is a set of formulas $\mathcal{S}$ such that $\mathcal{T}$ is the set of formulas in $\mathcal{L}$ that are provable from $\mathcal{S}$ using the deductive apparatus of $\mathcal{L}$.

Certain kinds of theories play an important role in the study of relation algebras. A theory is said to be *universal* if it has an axiomatization consisting of universal formulas. Similarly, a theory is said to be *universal Horn*, *conditional equational*, or *equational*, if it has an axiomatization consisting of universal Horn formulas, conditional equations, or equations respectively. The set of all formulas that are true in a class K of algebras is easily seen to be a theory. It is called the *elementary theory*, or the *first-order theory*, of K, and it is denoted by $Th(\mathsf{K})$.

Sometimes the word "theory" is used in a looser sense to refer to an arbitrary set of first-order formulas, or to a set of first-order formulas of some specific type. For example, the set of all universal formulas that are true in K is called the *universal theory* of K, the set of all universal Horn formulas that are true in K is called the *universal Horn theory* of K, the set of all conditional equations that are true in K is called the *conditional equational theory* of K, and the set of all equations that are true in K is called the *equational theory* of K. The latter is denoted by $Eq(\mathsf{K})$.

The theory of relation algebras is equational in nature: its axioms all have the form of equations, and the basic laws that are studied

have the form of equations or implications between equations. The deductive apparatus, and in particular the set of rules of inference, required for deriving equations from equations is much more elementary than the one required for deriving arbitrary first-order formulas. In fact, the following rules suffice. (1) *Tautology Rule*: every equation of the form $\sigma = \sigma$ is provable. (2) *Symmetry Rule*: from the equation $\sigma = \tau$, the equation $\tau = \sigma$ is provable. (3) *Transitivity Rule*: from equations $\sigma = \tau$ and $\tau = \gamma$, the equation $\sigma = \gamma$ is provable. (4) *Replacement Rule*: from equations $\sigma = \tau$ and $\gamma = \delta$, each of the equations

$$\sigma + \gamma = \tau + \delta, \qquad -\sigma = -\tau, \qquad \sigma\,;\gamma = \tau\,;\delta, \qquad \sigma^{\smile} = \tau^{\smile}$$

is provable. (5) *Substitution Rule*: from an equation $\varepsilon(v_0, \ldots, v_{n-1})$, each substitution instance $\varepsilon(\gamma_0, \ldots, \gamma_{n-1})$ obtained by simultaneously replacing each variable v_i with a term γ_i is provable.

In addition to its use in describing a certain type of first-order theory, the phrase *equational theory* is also used in a more restrictive sense to describe a set of equations that is closed under the relation of provability using the rules of inference (1)–(5). The sufficiency of these rules is captured in the *Completeness Theorem* for equational logic, which says that an equation ε is derivable from a set of equations $\mathcal{E}$ using the rules of inference (1)–(5) if and only if every model of $\mathcal{E}$ is also a model of ε.

2.5 Language of relations

There is another first-order language that is often used in the study of relation algebras. We call it the (*first-order* or *elementary*) *language of the theory of* (*binary*) *relations*, or more simply, the *language of relations*, and we denote it by $\mathcal{L}^*$. The logical symbols of $\mathcal{L}^*$ are the same as those of $\mathcal{L}$. The non-logical symbols of $\mathcal{L}^*$ consist of an unspecified number of binary relation symbols. For the purpose of illustration, it may be assumed for now that these relation symbols are enumerated in a sequence indexed by ordinal numbers: $\boldsymbol{R}_0, \boldsymbol{R}_1, \boldsymbol{R}_2, \ldots$. Occasionally, it is also advantageous to include a sequence of individual constant symbols (also called *operation symbols of rank zero*). We shall always state explicitly when such symbols are assumed to be present in the language. Again, for the purpose of illustration, it may be supposed

that these individual constant symbols, if any, are enumerated in a sequence indexed by ordinal numbers: $\boldsymbol{\alpha}_0, \boldsymbol{\alpha}_1, \boldsymbol{\alpha}_2, \ldots$. There are no operation symbols of rank higher than zero in $\mathcal{L}^*$.

The terms of $\mathcal{L}^*$ are the variables and the individual constant symbols, if any. The atomic formulas of $\mathcal{L}^*$ are the expressions of the form $\boldsymbol{R}_i\sigma\tau$ and the equations $\sigma = \tau$, where σ and τ are terms. Arbitrary formulas of $\mathcal{L}^*$ are built up from atomic formulas in exactly the same way as in $\mathcal{L}$.

A *relational structure* appropriate for this language is a system

$$\mathfrak{U} = (U,\, R_0,\, R_1,\, R_2, \ldots,\, \alpha_0,\, \alpha_1,\, \alpha_2, \ldots),$$

where R_i is a distinguished binary relation on the universe U for each index i, and α_j is a distinguished constant (that is to say, an element) in U for each index j. These relations and constants are the *interpretations* in $\mathfrak{U}$ of the relation symbols $\boldsymbol{R}_i$ and individual constant symbols $\boldsymbol{\alpha}_j$ in $\mathcal{L}^*$. Occasionally, we shall suppress explicit mention of the distinguished constants, and write simply

$$\mathfrak{U} = (U,\, R_0,\, R_1,\, R_2, \ldots).$$

The definition for $\mathcal{L}^*$ of the value of a term γ on a sequence r of n elements in $\mathfrak{U}$ is a simplified form of the definition for $\mathcal{L}$, as only a base clause is needed: the value of $\gamma(r)$ in $\mathfrak{U}$ is r_i when γ is a variable v_i, and it is the distinguished constant α_j when γ is the individual constant symbol $\boldsymbol{\alpha}_j$. The definition for $\mathcal{L}^*$ of the notion of a sequence r satisfying a formula Γ with variables among $v_0, \ldots, v_{n-1}$ in $\mathfrak{U}$ is very close to the definition for $\mathcal{L}$. Only the base clauses of the definition need to be extended in the following way: if Γ is an atomic formula of the form $\boldsymbol{R}_i\sigma\tau$, then the sequence r *satisfies* Γ in $\mathfrak{U}$ just in case the pair $(\sigma(r), \tau(r))$ belongs to the distinguished relation R_i. The remaining semantical notions such as truth and model are defined for $\mathcal{L}^*$ just as they are for $\mathcal{L}$.

2.6 Historical remarks

The idea of an axiomatic approach to the calculus of relations via a finite set of equational axioms goes back to Tarski [104]. In writing about a set-theoretical approach to the foundations of the theory of relations (see Chapter 1), he said the following.

> The above [set-theoretical] way of constructing the elementary theory of relations will probably seem quite natural to anyone who is familiar with modern mathematical logic. If, however, we are interested not in the whole theory of relations but merely in the calculus of relations, we must admit that this method has certain defects from the point of view of simplicity and elegance. We obtain the calculus of relations in a very roundabout way, and in proving theorems of this calculus we are forced to make use of concepts and statements which are outside the calculus. It is for this reason that I am going to outline another method of developing this calculus.
>
> In constructing the calculus of relations according to the second method we use only one kind of variables, namely relation variables, and we use the same constants as in the first method, with the exception of the quantifiers. [Tarski permitted the use of sentential connectives in [104], but avoided this usage in his later constructions of the calculus of relations.] From these constants and variables we construct relation designations exactly as before. In the construction of sentences, however, certain modifications are necessary on account of the absence of individual variables and quantifiers. As elementary sentences we take only sentences of the form 'R=S', where 'R' and 'S' stand for relation designations; and we form compound sentences from simpler ones by means of the connectives of the sentential calculus.
>
> Moreover we single out certain sentences which we call axioms. . . .

The set of axioms given in [104] is somewhat different from the one given in Definition 2.1. In particular, it is not equational in nature since sentential connectives are used. However, the possibility of giving an equational axiomatization of the calculus of relations is explicitly mentioned on p. 87 of [104]. The axiomatization given in Definition 2.1 was worked out by Tarski some time during the period 1942–1944, and was explicitly used by him in an unpublished manuscript dating from that period. A minor variant of this axiomatization was published in 1951 in Chin-Tarski [23].

The theory of Boolean algebras with operators was developed by Bjarni Jónsson and Tarski [54], and Lemmas 2.2–2.4 and 2.6 (in the more general forms given in Exercises 2.12–2.14 and 2.16) are due to them. Lemmas 2.5 and 2.7 (in the more general forms given in Exercises 2.15 and 2.17) are due to Givant. Also, Theorems 2.8 and 2.9 in their present form are due to Givant, but variants of them may have been known to others as well. There are, of course, versions of these theorems that apply to more general classes of Boolean algebras with complete operators. Also, there is a very close connection between Theorem 2.9 and a corresponding result regarding an axiomatization

of the class of atom structures of atomic relation algebras (see Chapter 19, in particular Theorems 19.12, 19.16, and 19.30).

The observation in Exercise 2.7 is explicitly made in Givant [34] (see Lemma 1.2 of that work). The results in Exercises 2.8 and 2.9 are due to Tarski; see Theorem 2.2 of [23]. The results in Exercises 2.18 and 2.19 are formulated in Theorem 1.5, and the subsequent remark, of Jónsson-Tarski [54]; but the proof given there for the case when the rank of the operation is greater than one is incorrect, as was pointed out by Richard Kramer. The correct proof given in the solutions section is due to Kramer.

Exercises

2.1. Prove that in any Boolean algebra (possibly with additional operations), if the supremum of every subset exists, then the infimum of every subset exists as well. Prove that, dually, if the infimum of every subset exists, then the supremum of every subset exists as well.

2.2. Prove that the following infinite associative laws hold in an arbitrary Boolean algebra (possibly with additional operations). Consider a system of index sets $(I_j : j \in J)$ with union I, and for each i in I, suppose that r_i is an element in the given Boolean algebra.

(i) If the sum $s_j = \sum_{i \in I_j} r_i$ exists for each index j in J, and if the sum $\sum_{j \in J} s_j$ exists, then the sum $\sum_{i \in I} r_i$ exists and

$$\textstyle\sum_{i \in I} r_i = \sum_{j \in J} s_j .$$

In other words, under the given hypotheses, we have

$$\textstyle\sum_{i \in I} r_i = \sum_{j \in J} \left(\sum_{i \in I_j} r_i \right) .$$

(ii) If the sum $s_j = \sum_{i \in I_j} r_i$ exists for each index j in J, and if the sum $\sum_{i \in I} r_i$ exists, then the sum $\sum_j s_j$ exists and

$$\textstyle\sum_{j \in J} s_j = \sum_{i \in I} r_i .$$

In other words, under the given hypotheses, we have

$$\textstyle\sum_{j \in J} \left(\sum_{i \in I_j} r_i \right) = \sum_{i \in I} r_i .$$

2.3. Prove that the following conditions on an element r in an arbitrary Boolean algebra (possibly with additional operations) are equivalent.

(i) r is an atom.
(ii) For every element s, either $r \leq s$ or $r \cdot s = 0$, but not both.
(iii) For every element s, either $r \leq s$ or $r \leq -s$, but not both.
(iv) $r \neq 0$, and whenever $r \leq s + t$, we have $r \leq s$ or $r \leq t$.
(v) $r \neq 0$, and whenever $r \leq \sum_i s_i$, we have $r \leq s_i$ for some i.

2.4. Prove that the following conditions on a Boolean algebra (possibly with additional operations) are equivalent.

(i) The algebra is atomic;
(ii) Every element in the algebra is the supremum of the set of atoms that it dominates;
(iii) The unit in the algebra is the supremum of the set of all atoms.

2.5. Prove that a non-degenerate atomless Boolean algebra (possibly with additional operations) is necessarily infinite.

2.6. The purpose of this and the next exercise is to show that (R10) and (R11) are equivalent on the basis of (R1)–(R3) and (R6)–(R9). Prove that the left-hand distributive law for relative multiplication,

$$r \,;(s+t) = r \,; s + r \,; t.$$

follows from (R6)—(R9). Use this law to derive the right-hand monotony law for relative multiplication,

$$s \leq t \qquad \text{implies} \qquad r \,; s \leq r \,; t.$$

2.7. Prove that (R10) is equivalent to the implication (R11) on the basis of the Boolean axioms (R1)–(R3) and the left-hand distributive law (or even just the right-hand monotony law) for relative multiplication (see Exercise 2.6).

2.8. Prove that (R10) is equivalent to the De Morgan-Tarski laws in the presence of the other axioms of relation algebra.

2.9. Prove that an algebra $\mathfrak{A}$ (of the same similarity type as relation algebras) is a relation algebra if and only if the axioms (R1)–(R5) and the De Morgan-Tarski laws hold in $\mathfrak{A}$. This gives an alternative (non-equational) axiomatization of the theory of relation algebras.

2.10. Complete the proof of Theorem 2.8 by treating each of the axioms (R4)–(R7).

2.11. Assuming the hypotheses of Theorem 2.8 on an algebra $\mathfrak{A}$ (of the same similarity type as relation algebras), give a simple set of necessary and sufficient conditions for $\mathfrak{A}$ to be a relation algebra when $\smile$ is the identity function on the set of atoms. Do the same when the operation $;$ is commutative on the set of atoms. What if $\smile$ is the identity function, and $;$ is commutative, on the set of atoms?

2.12. Prove Lemma 2.2 for an operation of arbitrary rank $n > 0$.

2.13. Prove Lemma 2.3 for an operation of arbitrary rank $n > 0$.

2.14. Prove Lemma 2.4 for an operation of arbitrary rank $n > 0$.

2.15. Prove Lemma 2.5 for an operation of arbitrary rank $n > 0$.

2.16. Prove Lemma 2.6 for an operation of arbitrary rank $n > 0$.

2.17. Prove Lemma 2.7 for an operation of arbitrary rank $n > 0$.

2.18. Let $(A\,,+\,,-)$ be a Boolean algebra.

(i) Prove that a unary operation f on A is distributive (or quasi-completely distributive) if and only if there is a normal and distributive (or quasi-completely distributive) operation g on A and an element t in A such that

$$f(r) = g(r) + t$$

for all elements r in A.

(ii) Prove that a binary operation f on A is distributive (or quasi-completely distributive) if and only if there is a normal and distributive (or quasi-completely distributive) operation g on A, two unary normal and distributive (or quasi-completely distributive) operations h and k on A, and an element t in A such that

$$f(r, s) = g(r, s) + h(r) + k(s) + t$$

for all elements r and s in A.

2.19. Formulate and prove a version of Exercise 2.18 that applies to distributive (or quasi-completely distributive) operations of arbitrary ranks $n \geq 1$.

2.20. Prove that Theorem 2.8 continues to hold if references to completely distributivity and to atoms are replaced by references to quasi-completely distributivity and to quasi-atoms respectively.

Chapter 3
Examples of relation algebras

Interesting and important examples of relation algebras may be constructed in a variety of ways: from sets of binary relations, from sets of Boolean matrices, from sets of formulas, from Boolean algebras, from groups, from projective geometries, from modular lattices, and from relatively small abstract algebraic structures. In this chapter we shall look at some of these constructions.

3.1 Set relation algebras

The classic example motivating the entire theory of relation algebras is the algebra of all relations on a set U. The universe of this algebra is the set of all (binary) relations on U. The operations of the algebra are union, complement (with respect to the universal relation $U \times U$), relational composition, and converse. The distinguished constant is the identity relation id_U on U. The algebra is called the *full set relation algebra on* U, or the *algebra of all relations on* U, and it is denoted by $\mathfrak{Re}(U)$.

A more general set-theoretic example is obtained by allowing the universe to be an arbitrary set of relations on U that contains the universal relation $U \times U$ and the identity relation id_U, and that is closed under the operations of union, complement (with respect to $U \times U$), relational composition, and converse. Such an algebra is called a *set relation algebra on* U, or a *proper relation algebra on* U, or an *algebra of relations on* U. Alternatively, we may also speak of a *square* set relation algebra, because the unit $U \times U$ is a Cartesian square. Arguments

S. Givant, *Introduction to Relation Algebras*,
DOI 10.1007/978-3-319-65235-1_3

similar to the ones given in Section 1.3 show that every proper relation algebra on a set satisfies Axioms (R1)–(R10).

A still more general example is obtained by allowing the universe to be an arbitrary set A of relations on U that contains a largest relation E and the identity relation id_U, and that is closed under the operations of union, complementation with respect to E (that is to say, if R is in A, then so is $E \sim R$), relational composition, and converse. Set-theoretic arguments similar to those in Section 1.3 show that the algebra

$$\mathfrak{A} = (A\,,\,\cup\,,\,\sim\,,\,|\,,\,{}^{-1}\,,\,id_U\,)$$

(complements being formed with respect to E) satisfies (R1)–(R10). The algebra is called a *set relation algebra*, or a *proper relation algebra*, or an *algebra of relations*, and U is called the *base set* of $\mathfrak{A}$. The largest relation E in $\mathfrak{A}$ must in fact be an equivalence relation on U. Indeed, the relations id_U, E^{-1}, and $E\,|\,E$ all belong to A, because of the assumption that A contains id_U and E, and is closed under converse and composition. Consequently, these three relations are all included in the largest relation E, which implies that E is a reflexive, symmetric, and transitive relation, by the remarks at the beginning of Section 1.4. A concrete example may be obtained by selecting an arbitrary equivalence relation E on U, and taking A to be the set of all relations on U that are included in E. The resulting algebra is called the *full set relation algebra on* E, or the *full algebra of relations on* E, and is denoted by $\mathfrak{Re}(E)$.

Among the various examples of square set relation algebras, there are four very simple ones that have a minimal number of relations. Fix an arbitrary set U, and consider the set A consisting of the empty relation $\varnothing$, the identity relation id_U, the diversity relation di_U, and the universal relation $U \times U$. It is obvious that A is closed under the Boolean operations of union and complement. The closure of A under converse is equally clear, since every relation in A is symmetric and therefore equal to its converse. The values of the operation of relational composition are completely determined on all but three pairs of relations in A, as Table 3.1 makes clear. The value in each of the three blank entries depends upon the size of the set U. If U has at most one element, then the relation di_U is empty, and in this case

$$di_U\,|\,di_U = di_U\,|(U \times U) = (U \times U)\,|\,di_U = \varnothing.$$

If U has at least two elements, then

$\mid$	$\varnothing$	id_U	di_U	$U \times U$
$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
id_U	$\varnothing$	id_U	di_U	$U \times U$
di_U	$\varnothing$	di_U		
$U \times U$	$\varnothing$	$U \times U$		$U \times U$

Table 3.1 Relational composition table for minimal square set relations algebras.

$$di_U \,|(U \times U) = (U \times U) \,|\, di_U = U \times U,$$

and in this case the only entry in the table that remains undetermined is that of $di_U \,|\, di_U$. The value of this last entry is id_U when U has two elements, and $U \times U$ when U has at least three elements. In any case, the set A is closed under composition, and is therefore the universe of a set relation algebra $\mathfrak{A}$ on U.

The structure of $\mathfrak{A}$ does not depend on the particular elements that belong to the base set U, but rather on the number of these elements. When U is empty, the four relations in A all coincide—they are all empty—and $\mathfrak{A}$ has just one element. When U has one element, the relations $\varnothing$ and di_U coincide, as do the relations id_U and $U \times U$, so that $\mathfrak{A}$ has exactly two elements. When U has at least two elements, the four relations in A are distinct from one another, so that $\mathfrak{A}$ is a set relation algebra with four elements. There are two possibilities in this case. For sets U with at least three elements, the corresponding set relation algebras all have the same composition table, irrespective of the size of U, since the entry for $di_U \,|\, di_U$ is always $U \times U$; these algebras are therefore all structurally the same. If U has exactly two elements, however, then the entry for $di_U \,|\, di_U$ in the composition table is not $U \times U$, but rather id_U, so that these algebras are structurally different from the others.

Summarizing, there are (up to isomorphism) exactly four set relation algebras that are obtained by taking the universe to be the smallest possible set of relations (on a set U) that contains the identity relation and is closed under the basic operations of union, complement (with respect to the universal relation $U \times U$), composition, and converse. We denote these *minimal* set relation algebras by $\mathfrak{M}_0$, $\mathfrak{M}_1$, $\mathfrak{M}_2$, and $\mathfrak{M}_3$, according to whether U has zero, one, two, or at least three elements respectively. The algebra $\mathfrak{M}_0$ is the only one of the four in which the equation $0 = 1$ is valid, and up to isomorphism it is characterized by

the validity of this equation. Algebras in which this equation is valid are said to be *degenerate*, because they have exactly one element and all of the operations are constant. The remaining three algebras are distinguished from one another by the value of the term 0’ ; 0’. More precisely, in $\mathfrak{M}_1$, $\mathfrak{M}_2$, and $\mathfrak{M}_3$ we respectively have

$$0\text{'} ; 0\text{'} = 0, \qquad 0\text{'} ; 0\text{'} = 1\text{'}, \qquad \text{and} \qquad 0\text{'} ; 0\text{'} = 1.$$

3.2 Matrix algebras

Another classic example motivating the theory of relation algebras is the algebra of Boolean matrices on a set U. The universe of this algebra is the set of all U-by-U Boolean matrices; the operations of the algebra are (coordinatewise) addition and complementation of matrices, and matrix multiplication and transposition; and the distinguished constant is the identity matrix (see Section 1.5). The algebra is called the *matrix algebra on* U, and it is denoted by $\mathfrak{Ma}(U)$.

As was observed in Section 1.5, the Boolean part of a matrix algebra is a direct power of the two-element Boolean algebra, so obviously axioms (R1)–(R3) are valid. Axioms (R4)–(R9) express well-known laws governing matrix multiplication, matrix transposition, and addition, laws that are taught in every introductory course on linear algebra. For instance, (R4) says that matrix multiplication is an associative operation, while (R7) says that for matrices M and N, the transpose of the matrix product $M \odot N$ coincides with the matrix product of the transposes N^{T} and M^{T}, in symbols,

$$(M \odot N)^{\mathrm{T}} = N^{\mathrm{T}} \odot M^{\mathrm{T}}.$$

The only axiom whose verification in a matrix algebra $\mathfrak{Ma}(U)$ presents any difficulty is (R10). An indirect proof of its validity may be obtained by observing that the axiom is valid in the full set relation algebra $\mathfrak{Re}(U)$ (see Section 1.3). Thus, for any relations R and S on U,

$$[R^{-1} \mid {\sim}(R \mid S)] \cup {\sim}S = {\sim}S.$$

The function mapping each relation T on U to the associated matrix M_T preserves all of the standard operations, by the observations in Section 1.6 (see, in particular, the equivalences (1), (3), (5), and (6) in that section), so we at once obtain

$$[(M_R)^{\mathrm{T}} \odot -(M_R \odot M_S)] + -M_S = -M_S.$$

Since the function mapping relations to corresponding matrices is a bijection, and therefore onto, the preceding implication implies that for any matrices M and N in $\mathfrak{Ma}(U)$,

$$[M^{\mathrm{T}} \odot -(M \odot N)] + -N = -N.$$

Thus, (R10) is valid in $\mathfrak{Ma}(U)$. The validity of the other relation algebraic axioms in $\mathfrak{Ma}(U)$ may be verified in a similar fashion. Conclusion: $\mathfrak{Ma}(U)$ is a relation algebra.

We shall see in Section 7.5 that the full set relation algebra $\mathfrak{Re}(U)$ and the matrix algebra $\mathfrak{Ma}(U)$ are really two sides of the same coin in the sense that they are isomorphic.

3.3 Formula relation algebras

The next examples of relation algebras are metamathematical in nature, and are constructed using the formulas in the elementary language $\mathcal{L}^*$ of relations (see Section 2.5). Consider the set $\mathcal{F}$ of all formulas in $\mathcal{L}^*$ that have at most two free variables, namely the first two variables $\boldsymbol{x}$ and $\boldsymbol{y}$ of $\mathcal{L}^*$. It is allowed that a formula in $\mathcal{F}$ may have just one free variable—either $\boldsymbol{x}$ or $\boldsymbol{y}$ — or even no free variables at all. If Γ is a formula in $\mathcal{F}$, and if u and v are variables in $\mathcal{L}^*$, then write $\Gamma(u, v)$ to denote the formula obtained from Γ by simultaneously substituting u and v for all free occurrences of $\boldsymbol{x}$ and $\boldsymbol{y}$ respectively, bound variables being changed to avoid collisions.

Fix a set $\mathcal{S}$ of formulas in $\mathcal{L}^*$, and define two formulas Γ and Δ in $\mathcal{F}$ to be *equivalent modulo* $\mathcal{S}$ if the sentence

$$\forall \boldsymbol{x} \forall \boldsymbol{y} (\Gamma \leftrightarrow \Delta)$$

is provable from the formulas in $\mathcal{S}$ using the deductive apparatus of $\mathcal{L}^*$. (If $\mathcal{S}$ is the empty set of formulas, then only the logical axioms and rules of inference of $\mathcal{L}^*$ are used in the proof, so in this case Γ and Δ are said to be *logically equivalent.*) It is easy to check that equivalence modulo $\mathcal{S}$ really is an equivalence relation on the set $\mathcal{F}$. Write $[\Gamma]$ for the equivalence class of a formula Γ. Let A be the set of equivalence classes of formulas in $\mathcal{F}$, and define on A two binary operations $+$

and ; , two unary operations $-$ and $\smile$, and a distinguished constant 1', as follows:

$$\begin{aligned} [\Gamma] + [\Delta] &= [\Gamma \vee \Delta], & -[\Gamma] &= [\neg\Gamma], \\ [\Gamma] ; [\Delta] &= [\exists \boldsymbol{z}(\Gamma(\boldsymbol{x}, \boldsymbol{z}) \wedge \Delta(\boldsymbol{z}, \boldsymbol{y}))], & [\Gamma]^{\smile} &= [\Gamma(\boldsymbol{y}, \boldsymbol{x})], \end{aligned}$$

for all formulas Γ and Δ in $\mathcal{F}$, and 1' is the equivalence class of the formula $\boldsymbol{x} = \boldsymbol{y}$ (where $=$ is the binary relation symbol for equality in $\mathcal{L}^*$). In other words, the sum and relative product of the equivalence classes of formulas Γ and Δ are defined to be the equivalence classes of the formulas

$$\Gamma \vee \Delta \qquad \text{and} \qquad \exists \boldsymbol{z}(\Gamma(\boldsymbol{x}, \boldsymbol{z}) \wedge \Delta(\boldsymbol{z}, \boldsymbol{y}))$$

respectively, and the complement and converse of the equivalence class of Γ are defined to be the equivalence classes of the formulas

$$\neg\Gamma \qquad \text{and} \qquad \Gamma(\boldsymbol{y}, \boldsymbol{x})$$

respectively. It is not difficult to verify that these operations on A are in fact well defined and that the resulting algebra

$$\mathfrak{A} = (A\,,\,+\,,\,-\,,\,;\,,\,^{\smile}\,,\,1')$$

is a relation algebra. It is called the *formula relation algebra of* $\mathcal{L}^*$ *modulo* $\mathcal{S}$, or the *formula relation algebra of* $\mathcal{S}$, for short.

To give a sense of how one proves that $\mathfrak{A}$ is a relation algebra, here are the verifications of Axioms (R7) and (R8). Let Γ and Δ be formulas in $\mathcal{F}$. According to the definition of the operations ; and $\smile$, the element $([\Gamma];[\Delta])^{\smile}$ is the equivalence class of the formula obtained from $\exists \boldsymbol{z}(\Gamma(\boldsymbol{x}, \boldsymbol{z}) \wedge \Delta(\boldsymbol{z}, \boldsymbol{y}))$ by simultaneously substituting $\boldsymbol{y}$ for $\boldsymbol{x}$, and $\boldsymbol{x}$ for $\boldsymbol{y}$—a substitution that may be indicated diagrammatically by writing $\boldsymbol{x} \mapsto \boldsymbol{y}$ and $\boldsymbol{y} \mapsto \boldsymbol{x}$. The (inductive) definition of substitution therefore implies that

$$([\Gamma] ; [\Delta])^{\smile} = [\exists \boldsymbol{z}(\Gamma(\boldsymbol{y}, \boldsymbol{z}) \wedge \Delta(\boldsymbol{z}, \boldsymbol{x}))].$$

Similarly,

$$\begin{aligned} [\Delta]^{\smile} ; [\Gamma]^{\smile} &= [\exists \boldsymbol{z}(\Delta(\boldsymbol{y}, \boldsymbol{x})(\boldsymbol{x}, \boldsymbol{z}) \wedge \Gamma(\boldsymbol{y}, \boldsymbol{x})(\boldsymbol{z}, \boldsymbol{y}))] \\ &= [\exists \boldsymbol{z}(\Delta(\boldsymbol{z}, \boldsymbol{x}) \wedge \Gamma(\boldsymbol{y}, \boldsymbol{z}))]. \end{aligned}$$

The notation $\Delta(\boldsymbol{y},\boldsymbol{x})(\boldsymbol{x},\boldsymbol{z})$ denotes the formula obtained by applying the substitution $\boldsymbol{x} \mapsto \boldsymbol{y}$ and $\boldsymbol{y} \mapsto \boldsymbol{x}$ to the formula Δ to obtain the intermediate formula $\Delta(\boldsymbol{y},\boldsymbol{x})$ (the equivalence class of which is the value of $[\Delta]^{\smile}$), and then applying the substitution $\boldsymbol{x} \mapsto \boldsymbol{x}$ and $\boldsymbol{y} \mapsto \boldsymbol{z}$ to the intermediate formula $\Delta(\boldsymbol{y},\boldsymbol{x})$. The result is a formula that is logically equivalent to the formula obtained by applying the composite substitution $\boldsymbol{x} \mapsto \boldsymbol{z}$ and $\boldsymbol{y} \mapsto \boldsymbol{x}$ to Δ, that is to say, it is logically equivalent to $\Delta(\boldsymbol{z},\boldsymbol{x})$. (The two formulas may differ in their bound variables, since a substitution can change some bound variables in order to avoid collisions between free and bound variables.) Similarly, the notation $\Gamma(\boldsymbol{y},\boldsymbol{x})(\boldsymbol{z},\boldsymbol{y})$ denotes the formula obtained by applying the substitution $\boldsymbol{x} \mapsto \boldsymbol{y}$ and $\boldsymbol{y} \mapsto \boldsymbol{x}$ to the formula Γ to obtain the intermediate formula $\Gamma(\boldsymbol{y},\boldsymbol{x})$ (the equivalence class of which is the value of $[\Gamma]^{\smile}$), and then applying the substitution $\boldsymbol{x} \mapsto \boldsymbol{z}$ and $\boldsymbol{y} \mapsto \boldsymbol{y}$ to the intermediate formula $\Gamma(\boldsymbol{y},\boldsymbol{x})$. The result is a formula that is logically equivalent to the formula obtained by applying the composite substitution $\boldsymbol{x} \mapsto \boldsymbol{y}$ and $\boldsymbol{y} \mapsto \boldsymbol{z}$ to Γ, that is to say, it is logically equivalent to the formula $\Gamma(\boldsymbol{y},\boldsymbol{z})$. Compare the formulas on the right sides of the equations, and use the (logically provable) commutativity of conjunction, to arrive at the desired conclusion:

$$([\Gamma]\,;[\Delta])^{\smile} = [\Delta]^{\smile}\,;[\Gamma]^{\smile}.$$

The verification of Axiom (R8) is similar. Let Γ, Δ, and Ω be formulas in $\mathcal{F}$. Apply the definitions of the operations $+$ and $;$, the definition of substitution, the (logically provable) distributivity of conjunction over disjunction, and the (logically provable) distributivity of existential quantification over disjunction to obtain

$$\begin{aligned}
([\Gamma]+[\Delta])\,;[\Omega] &= [\exists\boldsymbol{z}((\Gamma\vee\Delta)(\boldsymbol{x},\boldsymbol{z})\wedge\Omega(\boldsymbol{z},\boldsymbol{y}))]\\
&= [\exists\boldsymbol{z}((\Gamma(\boldsymbol{x},\boldsymbol{z})\vee\Delta(\boldsymbol{x},\boldsymbol{z}))\wedge\Omega(\boldsymbol{z},\boldsymbol{y}))]\\
&= [\exists\boldsymbol{z}((\Gamma(\boldsymbol{x},\boldsymbol{z})\wedge\Omega(\boldsymbol{z},\boldsymbol{y}))\vee(\Delta(\boldsymbol{x},\boldsymbol{z})\wedge\Omega(\boldsymbol{z},\boldsymbol{y})))]\\
&= [\exists\boldsymbol{z}(\Gamma(\boldsymbol{x},\boldsymbol{z})\wedge\Omega(\boldsymbol{z},\boldsymbol{y}))\vee\exists\boldsymbol{z}(\Delta(\boldsymbol{x},\boldsymbol{z})\wedge\Omega(\boldsymbol{z},\boldsymbol{y}))]\\
&= [\Gamma]\,;[\Omega]+[\Delta]\,;[\Omega].
\end{aligned}$$

3.4 Boolean relation algebras

Examples of relation algebras can be constructed in a rather trivial way from Boolean algebras. Fix a Boolean algebra $(A\,,+\,,-)$, and

define operations $;$ and $\smile$, and a distinguished constant 1', as follows:

$$r \,;\, s = r \cdot s, \qquad r^{\smile} = r, \qquad 1\text{'} = 1$$

for all r and s in A. The resulting algebra

$$\mathfrak{A} = (A\,,\, +\,,\, -\,,\, ;\,,\, {}^{\smile}\,,\, 1\text{'})$$

is easily seen to be a relation algebra. For example, the validity of the associative, distributive, and identity laws for relative multiplication in $\mathfrak{A}$—that is to say, the validity of (R4), (R8), and (R5)—follows directly from the validity of the corresponding laws for (Boolean) multiplication. Axioms (R6), (R7), and (R9) are trivially true in $\mathfrak{A}$, because converse is defined to be the identity operation on A and multiplication is commutative. The only axiom whose validity in $\mathfrak{A}$ is not immediately obvious is (R10). In view of the definition of the operations $;$ and $\smile$, the verification of (R10) reduces to checking the validity of the Boolean inequality

$$r \cdot -(r \cdot s) \leq -s,$$

and this is easy:

$$r \cdot -(r \cdot s) = r \cdot (-r + -s) = (r \cdot -r) + (r \cdot -s) = 0 + r \cdot -s \leq -s.$$

A relation algebra in which relative multiplication, converse, and the identity element satisfy the three defining equations given above is called a *Boolean relation algebra*. Here is a useful characterization of these algebras.

Lemma 3.1. *The following conditions on a relation algebra* $\mathfrak{A}$ *are equivalent.*

(i) $\mathfrak{A}$ *is a Boolean relation algebra.*
(ii) *Relative multiplication in* $\mathfrak{A}$ *coincides with multiplication.*
(iii) *The identity element in* $\mathfrak{A}$ *coincides with the unit.*

Proof. Condition (i) obviously implies condition (ii). The proof that condition (ii) implies condition (iii) is easy: if condition (ii) holds, then

$$1 = 1 \,;\, 1\text{'} = 1 \cdot 1\text{'} = 1\text{'},$$

by the identity law (R5), condition (ii), and the fact that every element in $\mathfrak{A}$ is below 1. The proof that condition (iii) implies condition (i)

is somewhat more involved. We make use of the following relation algebraic laws that will be proved in Lemma 5.20(i):

$$r \leq 1\text{'} \quad \text{and} \quad s \leq 1\text{'} \quad \text{implies} \quad r^{\smile} = r \quad \text{and} \quad r\,;s = r \cdot s. \tag{1}$$

Suppose now that condition (iii) holds for a relation algebra $\mathfrak{A}$. For any elements r and s in $\mathfrak{A}$, we have

$$r \leq 1 = 1\text{'} \qquad \text{and} \qquad s \leq 1 = 1\text{'},$$

by condition (iii), so $r^{\smile} = r$ and $r\,;s = r \cdot s$, by (1). Thus, condition (i) holds. □

Despite their trivial nature, Boolean relation algebras are quite useful. They are, in particular, a good source of examples. Since they are just notational variants of Boolean algebras, all results concerning Boolean algebras apply automatically to Boolean relation algebras. We shall see several examples of this later on. In the reverse direction, every notion and theorem about relation algebras has a Boolean algebraic version that is obtained by interpreting relative multiplication, converse, and the identity element as multiplication, the identity function, and the unit respectively. In fact, the Boolean algebraic version of such a theorem is an immediate consequence of the relation algebraic version. This observation applies in particular to every law in the theory of relation algebras: if relative multiplication and the identity element in such a law are replaced by multiplication and the unit respectively, and if all occurrences of converse are deleted, the result is a law in the theory of Boolean algebras.

3.5 Group complex algebras

Relation algebras can also be constructed from groups, and in fact this construction has played a very important role historically as a source of examples and problems in the theory of relation algebras. A *group* is an algebra

$$(G\,,\ \circ\,,\ ^{-1}\,,\ \iota)$$

with a binary operation $\circ$, a unary operation $^{-1}$, and a distinguished constant ι, in which the *associative law*, the *identity law*, and the *inverse law*,

$$f \circ (g \circ h) = (f \circ g) \circ h, \qquad f \circ \iota = \iota \circ f = f, \qquad f \circ f^{-1} = f^{-1} \circ f = \iota$$

respectively, hold for all elements f, g, and h in G. As is customary, we use the universe of a group to refer to the group itself.

Consider an arbitrary group G as above, and take A to be the set of all subsets of G. Obviously, A is closed under arbitrary unions and under complements (formed with respect to G). Define operations of *complex multiplication* and *complex inverse* by

$$X \,;\, Y = \{f \circ g : f \in X \text{ and } g \in Y\} \quad \text{and} \quad X^{\smile} = \{f^{-1} : f \in X\}$$

for all subsets X and Y of G, and take the distinguished element 1' to be the singleton of the group identity element, $\{\iota\}$. The resulting algebra

$$\mathfrak{A} = (A\,,\, +\,,\, -\,,\, ;\,,\, ^{\smile}\,,\, 1')$$

(where $+$ denotes the operation of forming the union of two subsets of G, and $-$ denotes the operation of forming the complement of a subset of G with respect to the unit element G) is a complete and atomic Boolean algebra with operations $;$ and $^{\smile}$ that are completely distributive for atoms, by their very definition. It is called the *complex algebra* of the group G, and is denoted by $\mathfrak{Cm}(G)$. The name stems from the fact that the elements of the algebra are the subsets—or, to use a somewhat archaic synonym, the *complexes*—of G.

Theorem 3.2. *The complex algebra of a group is a relation algebra.*

Proof. Let G be a group, and put $\mathfrak{A} = \mathfrak{Cm}(G)$. In order to show that $\mathfrak{A}$ is a relation algebra, it suffices to verify that (R4)–(R7) and (R11) hold for atoms in $\mathfrak{A}$, by Theorem 2.8. Here are the verifications of (R4) and (R11) as examples. The atoms in $\mathfrak{A}$ are the singletons of elements in G. Let f, g, and h be three such elements, and put

$$r = \{f\}, \qquad s = \{g\}, \qquad \text{and} \qquad t = \{h\}.$$

The definitions of these atoms, the definition of the operation $;$ in $\mathfrak{A}$, and the associative law for groups imply that

$$\begin{aligned} r \,;\, (s \,;\, t) &= \{f\} \,;\, (\{g\} \,;\, \{h\}) = \{f\} \,;\, \{g \circ h\} = \{f \circ (g \circ h)\} \\ &= \{(f \circ g) \circ h\} = \{f \circ g\} \,;\, \{h\} = (\{f\} \,;\, \{g\}) \,;\, \{h\} = (r \,;\, s) \,;\, t \end{aligned}$$

Thus, (R4) is valid for atoms in $\mathfrak{A}$.

The validity of (R11) for atoms in $\mathfrak{A}$ is a consequence of the following equivalences:

$$\begin{aligned}(r\,;s)\cdot t=0 \qquad &\text{if and only if} \quad \{f\circ g\}\cap\{h\}=\varnothing,\\ &\text{if and only if} \quad h\neq f\circ g,\\ &\text{if and only if} \quad f^{-1}\circ h\neq g,\\ &\text{if and only if} \quad \{f^{-1}\circ h\}\cap\{g\}=\varnothing,\\ &\text{if and only if} \quad (r^{\smile}\,;t)\cdot s=0. \qquad \Box\end{aligned}$$

The terminology *group relation algebra* is commonly employed to refer to the complex algebra of a group.

In order to simplify notation, the elements of a group are often identified with their singletons, provided no confusion can arise. In other words, an element f in G may often be treated as if it were an atom in $\mathfrak{Cm}(G)$, namely the atom $\{f\}$.

3.6 Geometric complex algebras

Important examples of relation algebras can also be constructed from projective geometries. A *projective geometry*—called here a *geometry*, for short—consists of a set of points, a set of lines, and a relation of incidence between the points and the lines, such that the following axioms hold. (1) Through any two distinct points, there passes one and only one line. (2) Every line has at least three points. (3) For distinct points p, q, s, and t, if the line through p and q intersects the line through s and t, then the line through p and s intersects the line through q and t (see Figure 3.1). Statements such as "a point p

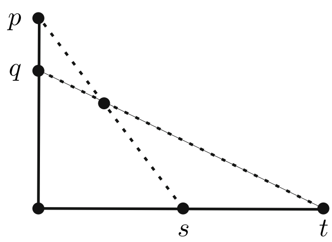


Fig. 3.1 The Pasch Axiom of projective geometry.

lies on a line ℓ" or "a line ℓ passes through a point p" mean that the point p is incident with the line ℓ. To say of two lines that they *intersect* means that there is a point incident with both lines. A set of points is said to be *collinear* if all of the points lie on one line. We shall follow the customary practice of using the set P of points in the geometry to refer to the entire geometry. The unique line through two distinct points r and s is usually denoted by rs. The third axiom above is often called the *Pasch Axiom*. Intuitively speaking, it says that if two lines ps and qt are coplanar in the sense that they lie in a common plane, namely the plane determined by the intersecting lines pq and st, then the lines ps and qt must intersect. (The plane determined by pq and st is defined to be the set of all points that lie on one of the lines intersecting pq and st in distinct points.) A classic and elementary result about projective geometries is that all lines in a given geometry P have the same number $m \geq 3$ of points; if $m = n+1$, then P is said to be of *order* n. For instance, if every line has exactly four points, then the order of P is three.

Fix a geometry P, and adjoin to P a new element ι (which we shall also call a "point") to form the set

$$P^+ = P \cup \{\iota\}.$$

The set A of all subsets of P^+ is obviously closed under arbitrary unions and under complements (formed with respect to P^+), and is therefore the universe of a complete and atomic Boolean set algebra. In order to simplify notation and reduce the number of braces, we shall follow the common geometric practice of identifying each point r with its singleton $\{r\}$, so that the points in P^+ may be thought of as coinciding with the atoms in A.

Define a function ; of two arguments from P^+ to A as follows: for each r in P, put

$$r\,;r = \begin{cases} \iota & \text{if} \quad P \text{ has order } 2, \\ \{\iota, r\} & \text{if} \quad P \text{ has order } > 2; \end{cases}$$

for distinct r and s in P, put

$$r\,;s = \{t \in P : t \text{ is collinear with, but distinct from, } r \text{ and } s\};$$

and for each r in P^+, put

$$r \,;\, \iota = \iota \,;\, r = r.$$

Extend $;$ to a binary operation on A by requiring it to be completely distributive for atoms:

$$X \,;\, Y = \bigcup\{r \,;\, s : r \in X \text{ and } s \in Y\}$$

for all subsets X and Y of P^+. The element ι (really the singleton of ι) acts as an identity element in A for the operation $;$ in the sense that

$$\iota \,;\, X = X \,;\, \iota = X,$$

so put $1' = \iota$. Define a unary operation $^\smile$ on A by

$$X^\smile = X$$

for all subsets X of P^+. The resulting algebra

$$\mathfrak{A} = (A\,,\, +\,,\, -\,,\, ;\,,\, {}^\smile\,,\, 1')$$

(where $+$ denotes the operation of forming the union of two subsets of P^+, and $-$ denotes the operation of forming the complement of a subset of P^+ with respect to the unit element P^+) is a complete and atomic Boolean algebra with operations $;$ and $^\smile$ that are completely distributive over atoms. We shall refer to $\mathfrak{A}$ as the *complex algebra* of the geometry P from which it is constructed, because the elements of the algebra are subsets, or complexes, of P^+ (P augmented by an identity point); and we shall denote $\mathfrak{A}$ by $\mathfrak{Cm}(P)$.

Theorem 3.3. *The complex algebra of a projective geometry is a relation algebra.*

Proof. Let P be a geometry, and write $\mathfrak{A} = \mathfrak{Cm}(P)$. In order to prove that $\mathfrak{A}$ is a relation algebra, it suffices, by Theorem 2.9, to check that conditions (i)–(iv) of that theorem are valid in $\mathfrak{A}$. In order to carry out this task, it is helpful to observe first that the operation $;$ is commutative. Indeed, $r \,;\, s = s \,;\, r$ is certainly true for atoms r and s in $\mathfrak{A}$, by the definition of $;$ on pairs of atoms, and this commutativity extends to arbitrary elements X and Y in $\mathfrak{A}$ by the definition of $;$ on pairs of subsets of P^+.

Conditions (ii)–(iv) of Theorem 2.9 are not difficult to check, using the definitions of the operations $;$ and $^\smile$ on atoms, and the

commutativity of $;$. Here, as an example, is the verification of condition (iv). Consider atoms r, s, and t in $\mathfrak{A}$, and assume as the hypothesis that $t \leq r ; s$. The argument splits into four cases. If r and s are distinct points in P, then the hypothesis and the definition of $;$ imply that t is a point collinear with, but distinct from, r and s. Consequently, s is a point that is collinear with, but distinct from, r and t, so

$$s \leq r ; t = r^{\smile} ; t,$$

by the definitions of $;$ and $^{\smile}$. If r and s are the same point in P, then the hypothesis and the definition of $;$ imply that t is ι when P has order two, and that t is either ι or r when P has order at least three. In either case, we obtain

$$s = r \leq r ; t = r^{\smile} ; t,$$

by the definitions of $;$ and $^{\smile}$. If $s = \iota$, then the hypothesis and the definition of $;$ imply that $t = r$. Consequently,

$$s = \iota \leq r ; r = r^{\smile} ; t,$$

by the definitions of $;$ and $^{\smile}$. Finally, if $r = \iota$, then the hypothesis and the definition of $;$ imply that $t = s$, so that

$$s = t = \iota ; t = r^{\smile} ; t.$$

The verifications of conditions (ii) and (iii) of Theorem 2.9 are very easy and are left as an exercise. Turn now to the verification of condition (i), or equivalently, to the verification of (R4) for atoms (see the proof of Theorem 2.9). Focus on the case when the order of the geometry P is at least three, so that each line has at least four points. Let r, s, and t be atoms in $\mathfrak{A}$. As might be expected, the argument splits into a number of cases. If at least one of the three atoms is ι, then the argument is trivial; for example, if $s = \iota$, then

$$r ; (s ; t) = r ; (\iota ; t) = r ; t = (r ; \iota) ; t = (r ; s) ; t.$$

Assume therefore that all three atoms are actually points in P. For conciseness, write $\mathrm{Col}\,(x, y, z)$ if x, y, and z are distinct collinear points in P.

Suppose first that the points r, s, and t are distinct. The definition of $;$ implies that

$$s\,;t = \{q : \mathrm{Col}\,(s,t,q)\},$$

and therefore

$$r\,;(s\,;t) = \bigcup\{r\,;q : \mathrm{Col}\,(s,t,q)\},$$

by the complete distributivity of the operation $;$. If r, s, and t are not collinear, then the preceding equation and the definition of $;$ imply that

$$r\,;(s\,;t) = \{p : \mathrm{Col}\,(r,q,p) \text{ for some } q \text{ such that } \mathrm{Col}\,(s,t,q)\}.$$

In geometric terms, this equation says that $r\,;(s\,;t)$ is the set of all those points p that lie on some line passing through r and intersecting the line st in a point different from s and t, with the points of intersection and the point r removed from the set. Because the points of intersection are different from s and t, the points on the lines rs and rt are all excluded from the set; and because the points of intersection are themselves removed from the set, the points on the line st are also excluded from the set. Thus, $r\,;(s\,;t)$ is the set of points lying in the plane through r, s, and t, but with the points on the lines rs, rt, and st all removed (see Figure 3.2). Since

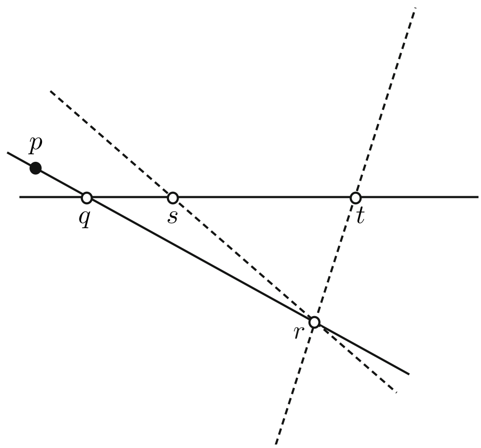


Fig. 3.2 The points in the set $r\,;(s\,;t)$.

$$(r\,;s)\,;t = t\,;(r\,;s) = t\,;(s\,;r),$$

by the commutativity of the operation $;$, the same argument with r and t interchanged shows that $(r\,;s)\,;t$ is the set of points lying in the

plane through t, s, and r, but with the points on the lines ts, tr, and sr all removed. Conclusion: the two sets of points $r\,;(s\,;t)$ and $(r\,;s)\,;t$ coincide, so the associative law

$$r\,;(s\,;t) = (r\,;s)\,;t$$

holds in this case.

If r, s, and t are collinear (but distinct), then the argument breaks into two subcases. When the order of the geometry P is three, the line st has four points—say q, r, s, and t—so that $s\,;t = \{q, r\}$ and therefore

$$r\,;(s\,;t) = (r\,;q) \cup (r\,;r) = \{s, t\} \cup \{r, \iota\} = \{r, s, t, \iota\}.$$

The commutativity of $;$, and the preceding argument with r and t interchanged, imply that

$$(r\,;s)\,;t = t\,;(r\,;s) = t\,;(s\,;r) = \{r, s, t, \iota\},$$

so the associative law holds in this case. When the order of the geometry is greater than three, there must be at least five points on the line st. The product $s\,;t$ is the set of all points on st that are different from s and t, and

$$r\,;(s\,;t) = (r\,;r) \cup \bigcup\{r\,;q : q \text{ lies on } st \text{ and } q \neq r, s, t\},$$

by the complete distributivity of $;$. There are at least two points—call them p and q—that lie on the line st and are distinct from r, s, and t. The product $r\,;p$ consists of all points on st except r and p, and in particular it contains the point q. The product $r\,;q$ consists of all points on st except r and q, and in particular it contains the point p. The product $r\,;r$ consists of r and ι. Consequently, the set $r\,;(s\,;t)$ consists of all points on the line st and the point ι. The commutativity of $;$, and the preceding argument with r and t interchanged, imply that $(r\,;s)\,;t$—which coincides with $t\,;(s\,;r)$—is the same set of points, so the associative law holds in this case as well.

There remain the cases when at least two of the three points r, s, and t are equal. Suppose $r = s \neq t$. The line st has at least four points, so there are two points on the line—call them p and q—that are different from s and t. The set $s\,;t$ includes these two points, so the set

$$r\,;(s\,;t) = s\,;(s\,;t)$$

includes the set $s ; p$, which consists of all points on st (including q) except s and p, and it includes the set $s ; q$, which consists of all points on st (including p) except s and q. Therefore, $r ; (s ; t)$ is the set of points on st that are different from s. On the other hand,

$$r ; s = s ; s = \{s, \iota\},$$

so

$$(r ; s) ; t = (s ; t) \cup (\iota ; t) = (s ; t) \cup \{t\}.$$

Thus, $(r ; s) ; t$ is also the set of points on st that are different from s, so the associative law holds in this case. The case $r \neq s = t$ reduces to the preceding case, by the commutativity of $;$, and the case $r = t$ (and s arbitrary) is a direct consequence of two applications of commutativity:

$$r ; (s ; t) = r ; (s ; r) = r ; (r ; s) = (r ; s) ; r = (r ; s) ; t.$$

This completes the verification of (an equivalent form of) condition (i) in Theorem 2.9. □

The names *Lyndon algebra* and *geometric relation algebra* are often used to refer to the complex algebra of a geometry or to the complex algebra of specific types of geometries.

A difficulty with the definition of relative multiplication for geometric complex algebras arises when one tries to apply it to a zero-dimensional geometry, that is to say, to a projective geometry consisting of a single point r. Such a geometry has no lines, so it is not clear what is meant by the order of the geometry. Does the (vacuously) true statement "every line has three points" apply, so that $r ; r = \iota$, or does the equally true statement "every line has more than three points" apply, so that $r ; r = \{\iota, r\}$? This seemingly innocuous and uninteresting case is important because it is desirable that all subgeometries (subspaces) of a geometry P of dimension at least one—including the zero-dimensional subgeometries—give rise to complex algebras with the same type of relative multiplication operation as $\mathfrak{Cm}(P)$. Perhaps the simplest and most direct way of resolving this dilemma is to associate with each geometry (in its list of fundamental notions) a *Boolean flag*—a unary relation that signals whether the order of the geometry is two or greater than two. For instance, if the geometry has order greater than two, the flag might be the set of all points in the geometry, while in the case of order two, it might be the empty set. Such

a flag would be inherited by subgeometries in the following sense: the flag of a subgeometry Q of P would, by definition, be the intersection of the flag of P with the set Q. Consequently, the flag of Q would be empty or the set of all points in Q, according to whether the flag of P was empty or the set of all points in P, that is to say, according to whether the order of P was equal to, or greater than, two. Under this conception, a zero-dimensional geometry of order two would not be isomorphic to a zero-dimensional geometry of order greater than two; but two zero-dimensional geometries of order greater than two would be isomorphic to one another. It follows that the complex algebra of a zero-dimensional geometry of order two would not be isomorphic to the complex algebra of a zero-dimensional geometry of order greater than two; but the complex algebras of two zero-dimensional geometries of order greater than two would be isomorphic to one another.

3.7 Lattice complex algebras

Relation algebras can also be constructed from modular lattices in a way that is strikingly similar to the construction of relation algebras from projective geometries. A lattice is a partially ordered set in which every two elements have a least upper bound and a greatest lower bound. Equivalently, a lattice is an algebra $(L\,,\,\vee\,,\,\wedge)$ with two binary operations $\vee$ and $\wedge$, called *join* and *meet* respectively, in which the *associative laws*, the *commutative laws*, the *idempotent laws*, and the *absorption laws*,

$$\begin{aligned} r\vee(s\vee t)&=(r\vee s)\vee t, &&\text{and} && r\wedge(s\wedge t)=(r\wedge s)\wedge t,\\ r\vee s&=s\vee r &&\text{and} && r\wedge s=s\wedge r,\\ r\vee r&=r &&\text{and} && r\wedge r=r,\\ r\vee(r\wedge s)&=r &&\text{and} && r\wedge(r\vee s)=r \end{aligned}$$

respectively, hold for all elements r, s, and t in L. The lattice is said to be *modular* if the *modular law*

$$r\le t \qquad \text{implies} \qquad r\vee(s\wedge t)=(r\vee s)\wedge t,$$

or equivalently,

$$t\le r \qquad \text{implies} \qquad r\wedge(s\vee t)=(r\wedge s)\vee t,$$

holds for all elements r, s, and t in L. The modular law may be written in the form of an equation instead of an implication:

$$(r \wedge t) \vee (s \wedge t) = [(r \wedge t) \vee s] \wedge t.$$

Consider a modular lattice $(L\,,\,\vee\,,\,\wedge)$ with a smallest element, called the *zero* of the lattice. The set A of all subsets of L is closed under arbitrary unions and under complements (formed with respect to the unit L), so it is the universe of a complete and atomic Boolean set algebra. As in the preceding two constructions, we shall identify each element r in L with its singleton $\{r\}$, so that the elements in L may be thought of as coinciding with the atoms in A.

Define a function $\,;\,$ of two arguments from L into A by

$$r\,;s = \{t \in L : r \vee t = s \vee t = r \vee s\}$$

for all elements r, s, and t in A, and extend $\,;\,$ to a binary operation on A by requiring it to be completely distributive for atoms:

$$X\,;Y = \bigcup\{r\,;s : r \in X \text{ and } s \in Y\}$$

for all subsets X and Y of L. Define a unary operation $\,^{\smile}\,$ on A by

$$X^{\smile} = X$$

for subsets X of L, and take 1' to be (the singleton of) the zero element in L. The resulting algebra

$$\mathfrak{A} = (A\,,\,+\,,\,-\,,\,;\,,\,^{\smile}\,,\,1')$$

(where $+$ denotes the operation of forming the union of two subsets of L, and $-$ denotes the operation of forming the complement of a subset of L with respect to the unit L) is a complete and atomic Boolean algebra with operations $\,;\,$ and $\,^{\smile}\,$ that are completely distributive over atoms. We shall refer to $\mathfrak{A}$ as the *complex algebra* of the lattice L, because the elements of $\mathfrak{A}$ are subsets, or complexes, of L; and we shall denote this algebra by $\mathfrak{Cm}(L)$.

Theorem 3.4. *The complex algebra of a modular lattice with zero is a relation algebra.*

Proof. Let L be a modular lattice with zero, and write $\mathfrak{A} = \mathfrak{Cm}(L)$. In order to prove that $\mathfrak{A}$ is a relation algebra, it suffices to verify that

conditions (i)–(iv) of Theorem 2.9 are valid in $\mathfrak{A}$. As a preliminary observation, notice that the commutativity of the join operation in L immediately implies the commutativity of the operation $\,;\,$ on atoms, and therefore on arbitrary elements in $\mathfrak{A}$.

Conditions (iii) and (iv) are very easy to check. For example, to verify condition (iii), assume that $t \leq r \,;\, s$. The operation $\,;\,$ is commutative, so we at once obtain $t \leq s \,;\, r$. Since $\,^\smile\,$ is defined to be the identity operation, this last inequality implies that $t^\smile \leq s^\smile \,;\, r^\smile$, as desired. The verification of condition (iv) is left as an exercise.

Turn now to the verification of condition (i), which is somewhat involved. Consider atoms p, r, s, and t in $\mathfrak{A}$, and assume that there is an atom q in $\mathfrak{A}$ such that

$$p \leq r \,;\, q \qquad \text{and} \qquad q \leq s \,;\, t. \tag{1}$$

The goal is to construct an atom $\bar{q}$ in $\mathfrak{A}$ such that

$$p \leq \bar{q} \,;\, t \qquad \text{and} \qquad \bar{q} \leq r \,;\, s. \tag{2}$$

By the convention regarding singletons, all of the atoms above may be viewed as elements in L, and consequently, in view of the definition of the operation $\,;\,$, the hypothesis in (1) and the goal in (2) may be translated into lattice-theoretic terms as follows: we assume

$$p \vee q = p \vee r = q \vee r, \tag{3}$$

$$q \vee s = q \vee t = s \vee t, \tag{4}$$

and we want to construct an element $\bar{q}$ in L such that

$$p \vee t = p \vee \bar{q} = t \vee \bar{q}, \tag{5}$$

$$r \vee \bar{q} = s \vee \bar{q} = r \vee s. \tag{6}$$

Take $\bar{q}$ to be the meet of one of the joins in (5) and one of the joins in (6), say

$$\bar{q} = (p \vee t) \wedge (r \vee s). \tag{7}$$

The derivations of equations (5) and (6) all have the same general form. They begin with an application of the definition in (7) and the modular law (sometimes with the implicit use of the associative and commutative laws for join), and they end with an application of the second absorption law (possibly with an implicit use of the associative

and commutative laws for join). In between the first two steps and the last step, the middle steps are based on the equations in (3) and (4) and the associative and commutative laws for join, applied in some order. To obtain the equality of the first and third terms in (5), the middle steps use (4), the commutative and associative laws, and (3):

$$\begin{aligned} t \vee \bar{q} = t \vee [(r \vee s) \wedge (p \vee t)] &= (t \vee r \vee s) \wedge (p \vee t) \\ &= (s \vee t \vee r) \wedge (p \vee t) = (q \vee t \vee r) \wedge (p \vee t) \\ &= (q \vee r \vee t) \wedge (p \vee t) = (p \vee q \vee t) \wedge (p \vee t) = p \vee t. \end{aligned}$$

To obtain the equality of the first and second terms in (5), the middle steps use the associative law, (3), and (4):

$$\begin{aligned} p \vee \bar{q} = p \vee [(r \vee s) \wedge (p \vee t)] &= (p \vee r \vee s) \wedge (p \vee t) \\ &= (p \vee q \vee s) \wedge (p \vee t) = (p \vee q \vee t) \wedge (p \vee t) = p \vee t. \end{aligned}$$

The derivations of the equations in (6) are analogous. To arrive at the equality of the second and third terms in (6), the middle steps use the commutative and associative laws, (4), and (3):

$$\begin{aligned} s \vee \bar{q} = s \vee [(p \vee t) \wedge (r \vee s)] &= (s \vee p \vee t) \wedge (r \vee s) \\ &= (p \vee s \vee t) \wedge (r \vee s) = (p \vee q \vee s) \wedge (r \vee s) \\ &= (p \vee r \vee s) \wedge (r \vee s) = r \vee s. \end{aligned}$$

To arrive at the equality of the first and third terms in (6), the middle steps use the commutative and associative laws, (3), and (4):

$$\begin{aligned} r \vee \bar{q} = r \vee [(p \vee t) \wedge (r \vee s)] &= (r \vee p \vee t) \wedge (r \vee s) \\ &= (p \vee r \vee t) \wedge (r \vee s) = (q \vee r \vee t) \wedge (r \vee s) \\ &= (q \vee t \vee r) \wedge (r \vee s) = (q \vee s \vee r) \wedge (r \vee s) = r \vee s. \end{aligned}$$

This completes the verification of condition (i).

Turn now to the verification of condition (ii), or equivalently, to the verification of (R5) for atoms (see the proof of Theorem 2.9). The distinguished constant 1' in $\mathfrak{A}$ is defined to be the zero element of the lattice, which is obviously an atom. By definition,

$$r \,;\, 1' = \{t \in L : r \vee t = 1' \vee t = r \vee 1'\} \tag{8}$$

for every atom r in $\mathfrak{A}$. Since

$$r \vee 1' = r \qquad \text{and} \qquad 1' \vee t = t,$$

it follows from (8) that $r \mathbin{;} 1' = r$ for atoms r in $\mathfrak{A}$. Thus, (R5) holds for atoms. □

It is worth pointing out that Theorem 3.4 essentially applies to all modular lattices, since every modular lattice L without a zero can be extended to a modular lattice with a zero simply by adjoining a new element to L and requiring this new element to be below every element in L.

In order to understand the definition of relative multiplication in the complex algebra of a modular lattice with zero, it is helpful to compare this definition with the definition of relative multiplication in the complex algebra of a projective geometry P. A *subspace* of P is a subset X that contains all of the points lying on any line determined by two points in X. In other words, if p and q are distinct points in X, and if r is any point lying on the line through p and q, then r also belongs to X. The set L of all subspaces of P is the universe of a lattice: the meet of two subspaces is defined to be their intersection, and the join of two subspaces is defined to be the intersection of all those subspaces of P that include the given two subspaces. Points in P are zero-dimensional subspaces, lines in P are one-dimensional subspaces, planes in P are two-dimensional subspaces, and so on. The empty set is the smallest subspace of P, and by convention it is assigned the dimension -1. The lattice L is modular, and it has a smallest element, namely the empty subspace.

The first observation to make is that the construction of $\mathfrak{Cm}(L)$ illuminates the role of the new element ι that must be adjoined to the geometry P in order to obtain an identity element in the complex algebra $\mathfrak{Cm}(P)$ (see Section 3.6). The points in the geometry P are essentially the elements in L that are zero-dimensional subspaces of P, and adjoining ι to P is tantamount to adjoining the empty subspace as a new element to P. The relative product of the empty subspace and a point p (a zero-dimensional subspace) in $\mathfrak{Cm}(L)$ is just p, which is the same as the relative product of the new element ι and p in $\mathfrak{Cm}(P)$.

The second observation concerns the difference between the complex algebras $\mathfrak{Cm}(L)$ and $\mathfrak{Cm}(P)$ with regards to the value of relative multiplication on zero-dimensional subspaces. Suppose r and s are distinct points in P. The relative product of r and s in the complex algebra $\mathfrak{Cm}(L)$ is the set

$$r\,;s=\{t\in L: r\vee t=s\vee t=r\vee s\}.$$

The subspace $r\vee s$ is the line passing through the points r and s, and the subspaces $t\vee r$ and $t\vee s$ are each equal to this line just in case the subspace t is either a point that is collinear with, but different from, the points r and s, or else t is the one-dimensional subspace that is the line through r and s. The relative product of the points r and s in the complex algebra $\mathfrak{Cm}(P)$ of the geometry P is the set

$$r\,;s=\{t\in P: t \text{ is collinear with, but distinct from, } r \text{ and } s\}.$$

Thus, the relative product of r and s in $\mathfrak{Cm}(L)$ contains one more element than it does in $\mathfrak{Cm}(P)$, namely the line passing through r and s.

The relative product of a point r with itself in $\mathfrak{Cm}(L)$ contains precisely two subspaces: the empty subspace and r itself. The same relative product in $\mathfrak{Cm}(P)$ consists of the element ι and the point r when the order of P is at least three, and it consists of just the identity element ι when the order of P is two. Thus, if P has order at least three, then the relative product of r with itself is essentially the same in $\mathfrak{Cm}(L)$ as it is in $\mathfrak{Cm}(P)$, but if P has order two, then this relative product contains one more element in $\mathfrak{Cm}(L)$ than it does in $\mathfrak{Cm}(P)$, namely the subspace r itself.

It may be helpful to give a few more examples of computations of relative products of atoms in $\mathfrak{Cm}(L)$. For the first example, observe that the relative product of any atom r with itself is always the set of all subspaces of P (that is to say, the set of all elements in L) that are included in r. For the second example, suppose that r is a point and s a line not passing through r. The join $r\vee s$ is the uniquely determined plane that contains both the point r and the line s. An element t in L belongs to $r\,;s$ just in case t is a subspace of the plane $r\vee s$ with the property that the join of t with each of r and s is equal to the plane. The element r is a point, and $t\vee r$ is a plane, so the subspace t cannot be empty or a point, nor can t be a line that contains the point r. The element s is a line, and $t\vee s$ is a plane, so t cannot coincide with the line s. Conclusion: t is either a line distinct from s that does not contain r, or else t is the entire plane $r\vee s$. For the third example, suppose r and s are distinct coplanar lines. The join $r\vee s$ is again the uniquely determined plane that includes both lines. An element t in L belongs to $r\,;s$ just in case t is a subspace of the plane $r\vee s$ with the property that the join of t with each of r and s is equal to the plane.

Consequently, t must be one of three types of subspaces: it can be a point in the plane that lies neither on r nor on s, or it can be a line in the plane that is distinct from both r and s, or it can be the entire plane $r \vee s$. For the last example, suppose r and s are lines that are not coplanar. The join $r \vee s$ is the uniquely determined three-dimensional space—call it p—that includes both lines. An element t in L belongs to $r\,;s$ just in case t is a subspace of p with the property that the join of t with each of r and s is equal to p. Because each of r and s is a line, and p is a three-dimensional space, the subspace t cannot be empty or a point, nor can t be a line that is coplanar with r or with s, nor can t be a plane that includes r or s. Thus, t is either a line included in the three-dimensional space p that is coplanar with neither r nor s, or it is a plane included in p that contains neither r nor s, or it is all of p.

Complex algebras of modular lattices are also called *Maddux algebras* or *lattice relation algebras*.

3.8 Small relation algebras

Occasionally, relation algebras are constructed by brute force methods (sometimes with the help of a computer). This approach is often applied to finite relation algebras with a small number of atoms, and proceeds in the following way. The set of atoms of a finite Boolean algebra is given, along with two tables, one specifying the relative product of each pair of atoms, and the other specifying the converse of each atom. The operations of relative multiplication and converse on atoms are extended to arbitrary elements in the Boolean algebra so as to be distributive for atoms. A proposed identity element is also specified. In order to prove that the resulting algebra is a relation algebra, it suffices by Theorem 2.8 to verify (R4)–(R7) and the implication in (R11) for atoms; alternatively, one can verify conditions (i)–(iv) of Theorem 2.9. In practice, (R5) and (R6) are usually trivial to verify, while (R4) and (R11) involve rather messy case arguments with a substantial number of cases.

Two concrete examples may serve to illustrate the main ideas of this method. Consider first a Boolean algebra $(A\,,\,+\,,\,-)$ with three atoms, say 1', s, and t. The relative product of two atoms and the converse of an atom are specified as in Table 3.2 and extended to all of A so as to be distributive. Write

;	1'	s	t
1'	1'	s	t
s	s	s	1
t	t	1	t

	$\smile$
1'	1'
s	t
t	s

Table 3.2 Relative multiplication and converse tables for atoms in $\mathfrak{A}$.

$$\mathfrak{A} = (A\,,\,+\,,\,-\,,\,;\,,\,^{\smile}\,,\,1\text{'})$$

for the resulting algebra. The column for 1' in the relative multiplication table shows that (R5) holds for all atoms, while the converse table makes clear that (R6) holds for all atoms.

The associative law (R4) for relative multiplication involves three variables, and there are three atoms in $\mathfrak{A}$, so in principle there are 27 cases to consider in order to verify this axiom for atoms. Some preliminary observations can reduce the number of cases considerably. Any case that involves 1' is trivial, because 1' is the identity element. For instance,

$$s\,;(1\text{'}\,;t) = s\,;t = (s\,;1\text{'})\,;t.$$

This observation reduces the number of cases that must be considered to eight. Also, the table for relative multiplication is symmetric across the diagonal, so relative multiplication between atoms (and therefore between any two elements) is commutative. The validity of one case of the associative law therefore implies the validity of all commuted versions of this case. For instance, the commutativity of relative multiplication alone implies that

$$s\,;(s\,;s) = (s\,;s)\,;s \qquad \text{and} \qquad s\,;(t\,;s) = (s\,;t)\,;s,$$

and also that

$$s\,;(s\,;t) = (s\,;s)\,;t \qquad \text{implies} \qquad t\,;(s\,;s) = (t\,;s)\,;s.$$

This reduces the number of cases that need to be considered to two. The definitions of relative multiplication and converse for atoms are symmetric with respect to the elements s and t in the sense that the correspondence mapping the atom 1' to itself and interchanging the atoms s and t extends to an automorphism of $\mathfrak{A}$. The validity of one case of the associative law therefore implies the validity of the corresponding case in which the roles of s and t are interchanged. For instance,

$$s\,;(s\,;t)=(s\,;s)\,;t \qquad \text{implies} \qquad t\,;(t\,;s)=(t\,;t)\,;s.$$

Finally, the relative product of any atom with 1 is 1. For instance,

$$s\,;1=s\,;(1\text{'}+s+t)=s\,;1\text{'}+s\,;s+s\,;t=s+s+1=1.$$

As a consequence of all of these observations, there is essentially only one case to consider when verifying (R4) for atoms, and this case is easily dealt with:

$$s\,;(s\,;t)=s\,;1=1=s\,;t=(s\,;s)\,;t.$$

Considerations similar to those involved in the verification of (R4) for atoms show that only two cases of (R7) for atoms need to be checked, and they are easy:

$$(s\,;s)^{\smile}=s^{\smile}=t=t\,;t=s^{\smile}\,;s^{\smile},$$

and

$$(s\,;t)^{\smile}=1^{\smile}=1=s\,;t=t^{\smile}\,;s^{\smile}.$$

The situation regarding the verification of (R11) is more complicated. Since all of the elements that need to be considered are atoms, it suffices to verify the form of (R11) that is given in condition (iv) of Theorem 2.9, namely

$$p\le q\,;r \qquad \text{implies} \qquad r\le q^{\smile}\,;p. \tag{1}$$

This implication involves three variables, so in principle there are again 27 cases to check. The preliminary observations made above reduce the number of cases considerably, but some care must be exercised. For instance, it is no longer true that every case in which one of the atoms is 1' is trivial. It seems easiest to proceed by considering first the various ways in which atoms can be assigned to the variables q and r, and then for each of these cases to treat the subcases that result from the various possible assignments of atoms to the variable p. If $q=1\text{'}$, then the hypothesis of (1) reduces to $p=r$, as does the conclusion, so (1) holds trivially. If $r=1\text{'}$, then the hypothesis of (1) reduces to $p=q$, and the conclusion to $1\text{'}\le q^{\smile}\,;q$. Since the relative product of each atom and its converse includes 1', the conclusion of (1) follows at once. If $r=q=s$, then $q\,;r=s\,;s=s$, so in this case we must have $p=s$. Since

$$q^{\smile} ; p = s^{\smile} ; s = t ; s = 1,$$

the conclusion of (1) again follows at once. If $q = t$ and $r = s$, then

$$q ; r = t ; s = 1.$$

The product $q^{\smile} ; p = s ; p$ includes s, and therefore r, for all three possible values of p, so the conclusion of (1) holds. The cases $q = r = t$ and $q = s$ and $r = t$ follow by the symmetry mentioned earlier. This completes the proof that $\mathfrak{A}$ is a relation algebra.

As the number of atoms of the given Boolean algebra increases, the verifications of the relation algebraic axioms for atoms become ever more complicated: in principle, the order of difficulty increases as the cube of the number of atoms. For instance, let $(A , + , -)$ be a Boolean algebra with four atoms, say 1', d, s, and t, and suppose that the relative product of two atoms and the converse of an atom are specified as in Table 3.3. Extend the operations ; and $^{\smile}$ to all

;	1'	d	s	t
1'	1'	d	s	t
d	d	$1' + s + t$	$d + s$	$d + t$
s	s	$d + s$	s	1
t	t	$d + t$	1	t

	$^{\smile}$
1'	1'
d	d
s	t
t	s

Table 3.3 Relative multiplication and converse tables for atoms in $\mathfrak{A}$.

of A so as to be distributive, and write

$$\mathfrak{A} = (A , + , - , ; , {}^{\smile} , 1')$$

for the resulting algebra. The verification of the associative law (R4) and condition (1) for atoms in principle now involve 64 cases each. However, several of the initial observations made about the algebra determined by Table 3.2 remain true of the algebra $\mathfrak{A}$ determined by Table 3.3, and simplify the verification task. For instance, if one of the atoms is 1', then the verification of the resulting statement is usually trivial, but some care must be exercised with regards to the verification of condition (1) in such cases. Also, relative multiplication is again commutative, so the validity of an equation under a certain assignment of atoms implies the validity of all commuted versions of this equation under the same assignment of atoms. Furthermore, the definitions of

relative multiplication and converse are again symmetric with respect to the atoms s and t in the sense that the correspondence mapping the atoms 1' and d to themselves and interchanging s and t extends to an automorphism of the algebra. Consequently any statement that is true for the atoms remains true when the elements s and t are interchanged. Finally, the relative product of any atom with 1 is 1.

With the help of these observations, the verification that $\mathfrak{A}$ is a relation algebra becomes manageable. For example, the 64 cases that are in principle needed in order to verify (R4) for atoms reduce to 4 essential cases that are easily checked:

$$\begin{aligned}
s ; (s ; t) &= s ; 1 = 1 = s ; t = (s ; s) ; t, \\
s ; (s ; d) &= s ; (d + s) = s ; d + s ; s = d + s = s ; d = (s ; s) ; d, \\
d ; (d ; s) &= d ; (d + s) = d ; d + d ; s = 1' + s + t + d = 1 \\
&= 1' ; s + s ; s + t ; s = (1' + s + t) ; s = (d ; d) ; s, \\
s ; (t ; d) &= s ; (d + t) = s ; d + s ; t = 1 = 1 ; d = (s ; t) ; d.
\end{aligned}$$

The initial observations also imply that the 16 cases needed in order to verify the second involution law (R7) for atoms can be reduced to four cases:

$$\begin{aligned}
(s ; s)^{\smile} &= s^{\smile} = t = t ; t = s^{\smile} ; s^{\smile}, \\
(d ; d)^{\smile} &= (1' + s + t)^{\smile} = 1'^{\smile} + s^{\smile} + t^{\smile} \\
&= 1' + t + s = d ; d = d^{\smile} ; d^{\smile}, \\
(s ; t)^{\smile} &= 1^{\smile} = 1 = s ; t = t^{\smile} ; s^{\smile}, \\
(s ; d)^{\smile} &= (d + s)^{\smile} = d^{\smile} + s^{\smile} = d + t = d ; t = d^{\smile} ; s^{\smile}.
\end{aligned}$$

The verifications of (R5) and (R6) for atoms are easy.

The verification of condition (1) for atoms also splits into 64 cases, but again there is a substantial reduction in the actual number of cases that need to be considered. If $q = 1'$, then the hypothesis and conclusion of (1) reduce to $p = r$, so (1) is trivially true in this case. If $r = 1'$, then the hypothesis of (1) reduces to $p = q$, and the conclusion reduces to $1' \leq q^{\smile} ; q$. The product $q^{\smile} ; q$ includes 1' for every atom q, so (1) holds in this case as well. There remain in principle nine cases to consider, one for each assignment of non-identity atoms to the variables q and r; but four of these cases can be deduced from the remaining five using the automorphism that interchanges s and t. In order to verify

each of the remaining five cases, assume the hypothesis of (1). If $q = t$ and $r = s$, then

$$q\,;r = t\,;s = 1,$$

so p can be any atom. The product

$$q^{\smile}\,;p = t^{\smile}\,;p = s\,;p$$

includes s—and therefore r—for any atom p, as a glance across the row for s in the right-hand table of Table 3.3 makes clear; so the conclusion of (1) holds in this case. If $q = r = s$, then

$$q\,;r = s\,;s = s,$$

so $p = s$ and

$$q^{\smile}\,;p = s^{\smile}\,;s = t\,;s = 1.$$

Clearly, the conclusion of (1) holds in this case. If $q = s$ and $r = d$, then

$$q\,;r = s\,;d = d + s,$$

so p is one of d and s, and therefore

$$q^{\smile}\,;p = s^{\smile}\,;p = t\,;p$$

is one of $t\,;d$ and $t\,;s$. Both of these products include d, which is r, so the conclusion of (1) holds. If $q = d$ and $r = s$, then p is again one of d and s, by the preceding case and the commutativity of the operation $;$, so

$$q^{\smile}\,;p = d^{\smile}\,;p = d\,;p$$

is either $d\,;d$ or $d\,;s$. Both of these products include s, which is r, so the conclusion of (1) holds in this case as well. Finally, if $q = r = d$, then

$$q\,;r = d\,;d = 1\text{'} + s + t,$$

so p is one of 1', s, and t, and

$$q^{\smile}\,;p = d^{\smile}\,;p = d\,;p$$

is one of $d\,;1\text{'}$, $d\,;s$, and $d\,;t$. Each of these products includes d and therefore r, so the conclusion of (1) holds in this last case.

The verifications of (R4), (R7), and condition (1) for atoms in the preceding two examples have been greatly simplified by two properties of the algebras under consideration: the commutativity of relative

multiplication and the existence of a non-trivial automorphism. As the number of atoms increases, the likelihood that a given constructed algebra will have one of these properties decreases, and therefore the chance of a substantial reduction in the number of distinct cases that must be treated is diminished. Little wonder, then, that small relation algebras with more than four atoms have for the most part been investigated with the aid of computers.

3.9 Independence of the axioms

An axiom in a given set of axioms is said to be *independent* of the remaining axioms in the set if it is not derivable from those axioms. A set of axioms is said to be *independent* if each of the axioms in the set is independent of the remaining axioms in the set. The standard method for establishing the independence of an axiom is to construct an *independence model* in which the axiom fails and the remaining axioms are valid. A classic example is the proof of the independence of the parallel postulate from the remaining axioms of Euclidean geometry via the construction of a model of non-Euclidean geometry. The problem of the independence of a given axiomatization of a theory is really a foundational question. If an axiom is shown to be dependent, then it is usually removed from the set of axioms and derived as a theorem in the subsequent axiomatic development of the theory.

From this perspective, it is natural to inquire whether the axiomatization of the theory of relation algebras given in Definition 2.1 is independent. This turns out to be the case. The proof follows the standard method outlined above: for each natural number $n = 1, \ldots, 10$, an algebra $\mathfrak{A}_n$ is constructed in which (Rn) fails and the remaining axioms hold. We demonstrate the method by showing that (R4), the associative law for relative multiplication, is independent of the remaining axioms.

To construct an independence model for (R4), start with a three-element partial algebra $(G\,,\,\circ\,,\,^{-1}\,,\,\iota)$, of the same similarity type as a group. The universe G of this partial algebra is the set $\{0, 1, 2\}$, the binary operation $\circ$ is determined by Table 3.4, the unary operation $^{-1}$ is the identity function on G, and the distinguished constant ι is 0. The values of $1 \circ 2$ and $2 \circ 1$ in the operation table for $\circ$ are left undefined. Form the complex algebra $\mathfrak{A}_4$ of this partial algebra in exactly the same

$\circ$	0	1	2
0	0	1	2
1	1	0	
2	2		0

Table 3.4 Table for the operation $\circ$.

way as the complex algebras of groups are formed. The operation of relative multiplication in $\mathfrak{A}_4$ is given by Table 3.5, while converse is the identity function on the universe of $\mathfrak{A}_4$, and $\{0\}$ is the identity element with respect to relative multiplication.

$;$	$\varnothing$	$\{0\}$	$\{1\}$	$\{2\}$	$\{0,1\}$	$\{0,2\}$	$\{1,2\}$	$\{0,1,2\}$
$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
$\{0\}$	$\varnothing$	$\{0\}$	$\{1\}$	$\{2\}$	$\{0,1\}$	$\{0,2\}$	$\{1,2\}$	$\{0,1,2\}$
$\{1\}$	$\varnothing$	$\{1\}$	$\{0\}$	$\varnothing$	$\{0,1\}$	$\{1\}$	$\{0\}$	$\{0,1\}$
$\{2\}$	$\varnothing$	$\{2\}$	$\varnothing$	$\{0\}$	$\{2\}$	$\{0,2\}$	$\{0\}$	$\{0,2\}$
$\{0,1\}$	$\varnothing$	$\{0,1\}$	$\{0,1\}$	$\{2\}$	$\{0,1\}$	$\{0,1,2\}$	$\{0,1,2\}$	$\{0,1,2\}$
$\{0,2\}$	$\varnothing$	$\{0,2\}$	$\{1\}$	$\{0,2\}$	$\{0,1,2\}$	$\{0,2\}$	$\{0,1,2\}$	$\{0,1,2\}$
$\{1,2\}$	$\varnothing$	$\{1,2\}$	$\{0\}$	$\{0\}$	$\{0,1,2\}$	$\{0,1,2\}$	$\{0\}$	$\{0,1,2\}$
$\{0,1,2\}$	$\varnothing$	$\{0,1,2\}$	$\{0,1\}$	$\{0,2\}$	$\{0,1,2\}$	$\{0,1,2\}$	$\{0,1,2\}$	$\{0,1,2\}$

Table 3.5 Operation table for relative multiplication in $\mathfrak{A}_4$.

To see that (R4) fails in $\mathfrak{A}_4$, take r to be the atom $\{1\}$, and take s and t to be the atom $\{2\}$, to obtain

$$r\,;(s\,;t) = \{1\}\,;(\{2\}\,;\{2\}) = \{1\}\,;\{0\} = \{1\},$$

and

$$(r\,;s)\,;t = (\{1\}\,;\{2\})\,;\{2\} = \varnothing\,;\{2\} = \varnothing.$$

Turn now to the proof that the remaining axioms of Definition 2.1 are valid in $\mathfrak{A}_4$. The Boolean part of $\mathfrak{A}_4$ is, by definition, a Boolean algebra of sets, so (R1)–(R3) are certainly valid in $\mathfrak{A}_4$. The operation of relative multiplication is commutative and distributive over addition in $\mathfrak{A}$, because $\circ$ is a commutative partial operation (see Table 3.4), and because the very definition of the complex operation $;$ in terms of $\circ$ (see Section 3.5) implies that it distributes over arbitrary sums.

From these observations, together with the fact that converse is the identity function on the universe of $\mathfrak{A}_4$, and $\{0\}$ is an identity element with respect to operation of relative multiplication, it easily follows that (R5)–(R9) all hold in $\mathfrak{A}_4$.

It must still be shown that (R10) is valid in $\mathfrak{A}_4$. Since (R1)–(R3) and (R6)–(R9) all hold in $\mathfrak{A}_4$, the validity of (R10) is equivalent to that of (R11), which in turn equivalent to that of condition (iv) in Theorem 2.9 (see the remarks following that theorem). In the present situation, the verification of condition (iv) reduces to showing that

$$t \leq r \,;\, s \qquad \text{implies} \qquad s \leq r \,;\, t \tag{1}$$

for all atoms r, s, and t. If r is the identity element $\{0\}$, then (1) reduces to the triviality that $t = s$ implies $s = t$. If s is the identity element, then the hypothesis of (1) reduces to $t = r$; in this case $r;t = r;r$, which is always the identity element when r is an atom (see Table 3.5), so the conclusion of (1) holds. It may therefore be assumed that r and s are atoms distinct from the identity element. If $r = s$, then the hypothesis of (1) is only satisfied if t is the identity element (see Table 3.5), and in this case the conclusion of (1) holds trivially. The only remaining case is when r and s are, in some order, the two subdiversity atoms $\{1\}$ and $\{2\}$. In this case the relative product $r \,;\, s$ is the empty set (see Table 3.5), so the hypothesis of (1) is never satisfied, and therefore the implication in (1) is always true.

	$^{-1}$
$\varnothing$	$\varnothing$
$\{0\}$	$\{0\}$
$\{1\}$	$\{2\}$
$\{2\}$	$\{1\}$
$\{0,1\}$	$\{0,2\}$
$\{0,2\}$	$\{0,1\}$
$\{1,2\}$	$\{1,2\}$
$\{0,1,2\}$	$\{0,1,2\}$

Table 3.6 Converse table for the complex algebra of the group of integers modulo 3.

The proofs that the remaining axioms in Definition 2.1 are also independent are similar in spirit to the preceding argument. In each case,

the most difficult step is the construction of a suitable independence model for the axiom under consideration. See [3] for details.

3.10 Historical remarks

Full set relation algebras on a set U are implicit in the work of Peirce and Schröder, although they did not conceive of algebras of relations in the same way that we think of them today. Set relation algebras in the more general sense discussed in Section 3.1, where the unit is an arbitrary equivalence relation, were proposed by Tarski. As Tarski well understood, the inclusion of these algebras into the class of set relation algebras implies that, up to isomorphism, the class is closed not only under subalgebras, but also under direct products.

The construction of formula relation algebras is due to Tarski, as are the results in Exercises 3.12–3.14. Boolean relation algebras go back to Tarski as well. In particular, Lemma 3.1 and the observation in Exercise 3.15 are due to him. The construction of group complex algebras is due to John Charles Chenoweth McKinsey, who initially called them *Frobenius algebras*—see [53].

The history of geometric complex algebras is somewhat involved. Jónsson [49] constructed examples of (non-representable) relation algebras from non-Desarguesian projective planes. His construction already contains most of the key ideas that are involved in the definitions of relative multiplication, converse, and the identity element for geometric complex algebras (see Section 3.6). He did not, however, have the current definition of the relative product of an element with itself, nor did he have the direct derivation of the associative law for relative multiplication from the axioms of projective geometry. Instead, his construction uses a transfinite inductive procedure to arrive at an algebra in which the associative law is valid.

Roger Conant Lyndon [70] substantially simplified Jónsson's construction, giving the definition of relative multiplication in these algebras that is used today, and giving a direct derivation of the associative law from the axioms of projective geometry, thereby obviating the need for a construction by transfinite induction. Lyndon also saw that his construction yields examples of relation algebras for every underlying projective geometry of dimension at least one. He characterized when such relation algebras are *completely representable* in the

sense that they are isomorphic to set relation algebras via mappings that preserves all sums as unions (see Theorem 17.14). Lyndon was motivated not only by Jónsson's construction, but also by a problem from Jónsson-Tarski [53], which asks whether every integral relation algebra—that is to say, every relation algebra in which the relative product of two non-zero elements is always non-zero—is embeddable into the complex algebra of a group. Lyndon considered only projective geometries of dimension at least one and order at least three, but he was aware of how to handle the cases of a projective geometry of order two and a projective geometry of dimension 0 or -1. (He seems not to have been aware of the need for a Boolean flag in the case dimension 0.) The theorem in Exercise 3.26 is essentially due to Lyndon [70]. The observation in Exercise 3.28 is from Jónsson [50].

Complex algebras of modular lattices with zero were created by Roger Duncan Maddux [73] in order to answer positively the question in Jónsson [49] of whether every modular lattice is isomorphic to the lattice of commuting equivalence elements of some relation algebra.

Small relation algebras were first investigated by Lyndon, who discovered that every finite relation algebra with at most three atoms is *representable* in the sense that it is isomorphic to a set relation algebra (see Footnote 13 on the last page of Lyndon [68]). The results in Exercises 3.2, 3.3, and 3.36–3.39 were certainly known to him, although he did not publish any statements or proofs of them. Lyndon's investigations of small relation algebras were extended to finite relation algebras with four atoms by Ralph Nelson Whitfield McKenzie [82], but McKenzie did not obtain a complete description of all such algebras, nor did he publish his results in this direction. He did, however, succeed in showing that there exist examples of finite relation algebras with four atoms that are not representable (see [82] and [83]). It is likely that the several of the examples in Exercises 3.40–3.41 were known to him. Stephen Comer used a computer to study and enumerate the integral relation algebras with four atoms—see [24] and [25]. Maddux continued these computer-aided investigations by enumerating the finite relation algebras with five atoms. In particular, his computer computations led him to the conclusion that there are 4527 finite, integral relation algebras with at most five atoms, and these algebras are enumerated in Maddux [78].

The construction of the independence model $\mathfrak{A}_4$ in Section 3.9 is due to McKinsey, who used it to prove in the early 1940s that the associative law for relative multiplication is independent of the remaining

relation algebraic axioms (see the appendix to Tarski [106]). Hyman Kamel [57] (see also Kamel [58]) presented an axiomatization of the theory of (simple) relation algebras different from the one given in Tarski [105], and proved its equivalence to Tarski's axiomatization (see Exercise 4.27). In addition, Kamel proved the independence of some of his axioms, but he was unable to establish the independence of all of them. Hajnal Andréka, Givant, Peter Jipsen, and István Németi have shown in [3] that all of the axioms in Definition 2.1 are independent of one another. Their independence models are different from the ones used by Kamel.

Exercises

3.1. Prove that all degenerate relation algebras are isomorphic.

3.2. Prove that every relation algebra with two elements must be isomorphic to $\mathfrak{M}_1$.

3.3. If E is the identity relation on a two-element set, then the Boolean set relation algebra $\mathfrak{Re}(E)$ has four elements. Prove that every four-element relation algebra is isomorphic to one of $\mathfrak{M}_2$, $\mathfrak{M}_3$, and $\mathfrak{Re}(E)$.

3.4. Verify that axioms (R4)–(R9) are valid in every matrix algebra by using the correspondence between relations and matrices.

3.5. Verify directly that axioms (R4)–(R10) are valid in every matrix algebra by using the definitions of the operations involved in each axiom.

3.6. Verify that (R4), (R5), (R6), (R9), and (R10) are valid in every formula relation algebra.

3.7. The construction of a formula relation algebra actually goes through for any first-order language $\mathcal{L}^*$, not just the language of relations, and for any set of formulas $\mathcal{S}$ in $\mathcal{L}^*$. Describe the details of this construction.

3.8. Let $\mathcal{L}$ be a language of first-order logic with one binary relation symbol $\boldsymbol{R}$, and suppose $\mathcal{S}$ is the set of sentences expressing that $\boldsymbol{R}$ is a *dense linear ordering without endpoints*. Thus, the sentences in $\mathcal{S}$ say that: (1) $\boldsymbol{R}$ is a strict ordering that is total in the sense that, for

any two elements, one is always greater than, equal to, or less than the other; (2) for any elements r and s, if r is smaller than s, then there is an element t that is greater than r and less than s; (3) there is no greatest and no least element. Describe the resulting formula relation algebra.

3.9. Let $\mathcal{L}$ be a language of first-order logic with one binary relation symbol $\boldsymbol{R}$, and suppose $\mathcal{S}$ is the set of sentences expressing that $\boldsymbol{R}$ is a *dense linear ordering*. Thus, the sentences in $\mathcal{S}$ say that: (1) $\boldsymbol{R}$ is a strict ordering that is total; (2) for any elements r and s, if r is smaller than s, then there is an element t that is greater than r and less than s. Describe the resulting formula relation algebra.

3.10. Let $\mathcal{L}$ be a language of first-order logic with one binary relation symbol $\boldsymbol{R}$, and suppose $\mathcal{S}$ is the set of sentences expressing that $\boldsymbol{R}$ is a permutation without cycles of a set with five elements. Describe the resulting formula relation algebra.

3.11. Let $\mathcal{L}$ be a language of first-order logic with one binary relation symbol $\boldsymbol{R}$, and suppose $\mathcal{S}$ is the set of sentences expressing that $\boldsymbol{R}$ is the successor function on the set of integers. Thus, the sentences in $\mathcal{S}$ say that $\boldsymbol{R}$ is a bijection without cycles. Describe the resulting formula relation algebra.

3.12. The notion of a *restricted formula relation algebra* is defined in a manner similar to that of a formula relation algebra (see Section 3.3), except that the set $\mathcal{F}$ of formulas in $\mathcal{L}^*$ having $\boldsymbol{x}$ and $\boldsymbol{y}$ as their only free variables is replaced by a more restricted set of formulas. Let $\mathcal{L}_3^*$ be the set of formulas in $\mathcal{L}^*$ that contain no variables (free or bound) different from $\boldsymbol{x}$, $\boldsymbol{y}$, and $\boldsymbol{z}$, and put

$$\mathcal{F}^* = \mathcal{F} \cap \mathcal{L}_3^*.$$

The set of formulas $\mathcal{F}^*$ is used instead of $\mathcal{F}$ to construct the restricted formula relation algebras of $\mathcal{L}^*$. In order to define an appropriate notion of substitution for the set of formulas $\mathcal{F}^*$, one must change bound variables in such a way that variables different from $\boldsymbol{x}$, $\boldsymbol{y}$, and $\boldsymbol{z}$ are not introduced. Supply the details of this construction, and prove that every restricted formula relation algebra is a relation algebra.

3.13. Prove that every set relation algebra is isomorphic to a restricted formula relation algebra (see Exercise 3.12).

3.14. Prove that every formula relation algebra is isomorphic to a set relation algebra.

3.15. Prove that every Boolean relation algebra is isomorphic to a subalgebra of $\mathfrak{Re}(id_U)$ for some set U. Conclude that every Boolean relation algebra is isomorphic to a set relation algebra.

3.16. Give an example of an atomless relation algebra.

3.17. Give an example of an atomless relation algebra that is simple in the sense that there are exactly two congruence relations on the algebra.

3.18. Complete the proof of Theorem 3.2 by showing that (R5)–(R7) hold for atoms in the complex algebra of a group.

3.19. Prove that the complex algebra of a group is isomorphic to a set relation algebra.

3.20. A relation algebra is called *integral* if $r\,;s = 0$ always implies that $r = 0$ or $s = 0$. Prove that the complex algebra of a group is integral.

3.21. Prove that conditions (ii) and (iii) of Theorem 2.9 hold in the complex algebra of a projective geometry of order at least three.

3.22. It was shown in the proof of Theorem 3.3 that an equivalent form of condition (i) from Theorem 2.9, namely the associative law for atoms, is true in the complex algebra of a geometry of order at least three. Prove directly that condition (i) itself holds in this algebra.

3.23. Prove that conditions (i)–(iii) of Theorem 2.9 hold in the complex algebra of a projective geometry of order two.

3.24. Prove that the complex algebra of a geometry is an integral relation algebra in the sense defined in Exercise 3.20.

3.25. Prove that in the complex algebra of a geometry of order two, if relative multiplication is defined exactly as in the case of order at least three, then the associative law fails.

3.26. Prove that a relation algebra $\mathfrak{A}$ is isomorphic to the complex algebra of a geometry of order at least three if and only if the following conditions hold.

(i) $\mathfrak{A}$ is complete and atomic.
(ii) 1’ is an atom.
(iii) $p^{\smile} = p$ for every atom p in $\mathfrak{A}$.
(iv) $p \mathbin{;} p = p + 1’$ for every atom $p \neq 1’$.

3.27. Prove that a relation algebra $\mathfrak{A}$ is isomorphic to the complex algebra of a geometry of order two if and only if the following conditions hold.

(i) $\mathfrak{A}$ is complete and atomic.
(ii) 1’ is an atom.
(iii) $p^{\smile} = p$ for every atom p in $\mathfrak{A}$.
(iv) $p \mathbin{;} p = 1’$ for every atom p.

3.28. Prove that in the complex algebra of a projective line of order at least three, the equation $r \mathbin{;} r = r \mathbin{;} r \mathbin{;} r$ is true.

3.29. Prove that the complex algebra of a zero-dimensional geometry of order two is not isomorphic to the complex algebra of a zero-dimensional geometry of order greater than two, but the complex algebras of two zero-dimensional geometries of order greater than two are isomorphic to one another.

3.30. Prove that the complex algebra of a modular lattice is an integral relation algebra in the sense defined in Exercise 3.20.

3.31. Complete the proof of Theorem 3.4 by verifying that condition (iv) from Theorem 2.9 is valid in $\mathfrak{A}$.

3.32. Suppose L is the lattice of all subspaces of some projective geometry. Let r and s be elements in L and therefore atoms in $\mathfrak{Cm}(L)$. Describe the elements that belong to the relative product $r \mathbin{;} s$ in each of the following cases.

(i) r is a line and s is a point lying on r.
(ii) r is a plane and s is a point lying in r.
(iii) r is a plane and s is a point not lying in r.
(iv) r is a plane and s is a line lying in r.
(v) r is a plane and s is a line not lying in r.
(vi) r and s are distinct planes.

3.33. For the algebra $\mathfrak{A}$ discussed in the second example of Section 3.8, prove that the first equation below implies all of the remaining equations.

$$s\,;(t\,;d) = (s\,;t)\,;d, \qquad t\,;(s\,;d) = (t\,;s)\,;d,$$
$$s\,;(d\,;t) = (s\,;d)\,;t, \qquad t\,;(d\,;s) = (t\,;d)\,;s,$$
$$d\,;(s\,;t) = (d\,;s)\,;t, \qquad d\,;(t\,;s) = (d\,;t)\,;s.$$

3.34. For the algebra $\mathfrak{A}$ discussed in the second example of Section 3.8, prove that the first equation below implies all of the remaining equations.

$$(s\,;d)^{\smile} = d^{\smile}\,;s^{\smile}, \qquad (t\,;d)^{\smile} = d^{\smile}\,;t^{\smile},$$
$$(d\,;s)^{\smile} = s^{\smile}\,;d^{\smile}, \qquad (d\,;t)^{\smile} = t^{\smile}\,;d^{\smile}$$

3.35. For the algebra $\mathfrak{A}$ discussed in the second example of Section 3.8, assume that for every atom p in $\mathfrak{A}$, the inequality $p \le s\,;d$ implies the inequality $d \le s^{\smile}\,;p$. What other cases of condition (1) for atoms can be easily derived from this case?

3.36. Let $(A\,,+\,,-)$ be a Boolean algebra with eight elements and three atoms, 1’, s, and t. Define every atom to be its own converse. If the relative multiplication table for atoms is any one of the following (where 0’ $= s+t$), prove that the resulting algebra is a relation algebra.

(i)

;	1’	s	t
1’	1’	s	t
s	s	1’	t
t	t	t	1’ $+ s$

(ii)

;	1’	s	t
1’	1’	s	t
s	s	1’ $+ s$	t
t	t	t	1’ $+ s$

(iii)

;	1’	s	t
1’	1’	s	t
s	s	1’	t
t	t	t	1

(iv)

;	1’	s	t
1’	1’	s	t
s	s	1’ $+ s$	t
t	t	t	1

(v)

;	1’	s	t
1’	1’	s	t
s	s	1’ $+ t$	0’
t	t	0’	1’ $+ s$

(vi)

;	1’	s	t
1’	1’	s	t
s	s	1’ $+ t$	0’
t	t	0’	1

(vii)

;	1'	s	t
1'	1'	s	t
s	s	1	0'
t	t	0'	1

3.37. Let $(A\,,+\,,-)$ be a Boolean algebra with eight elements and three atoms, 1', s, and t. Define 1' to be its own converse, and define the converses of s and t to be t and s respectively. If the relative multiplication table for atoms is as in (i) or (ii) (where 0' $= s+t$), prove that the resulting algebra is a relation algebra.

(i)

;	1'	s	t
1'	1'	s	t
s	s	t	1'
t	t	1'	s

(ii)

;	1'	s	t
1'	1'	s	t
s	s	0'	1
t	t	1	0'

3.38. Let $(A\,,+\,,-)$ be a Boolean algebra with eight elements and three atoms, r, s, and t. Define every atom to be its own converse. If the relative multiplication table for atoms is (i), (ii), or (iii), prove that the resulting algebra is a relation algebra.

(i)

;	r	s	t
r	r	0	0
s	0	s	0
t	0	0	t

(ii)

;	r	s	t
r	r	0	0
s	0	s	t
t	0	t	s

(iii)

;	r	s	t
r	r	0	0
s	0	s	t
t	0	t	$s+t$

3.39. Prove that, up to isomorphism, there are no other relation algebras with eight elements and three atoms except the algebra $\mathfrak{A}$ in the first example of Section 3.8 and the algebras in Exercises 3.36–3.38.

3.40. Let $(A\,,+\,,-)$ be a Boolean algebra with sixteen elements and four atoms, 1', d, s, and t. Define every atom to be its own converse. If the relative multiplication table for atoms is any one of the following (where 0' $= d+s+t$), prove that the resulting algebra is a relation algebra.

(i)

;	1'	d	s	t
1'	1'	d	s	t
d	d	1'	t	s
s	s	t	1'	d
t	t	s	d	1'

(ii)

;	1'	d	s	t
1'	1'	d	s	t
d	d	$1' + s + t$	0'	0'
s	s	0'	$1' + d$	$d + t$
t	t	0'	$d + t$	1

(iii)

;	1'	d	s	t
1'	1'	d	s	t
d	d	1'	t	s
s	s	t	$1' + s$	$d + t$
t	t	s	$d + t$	$1' + s$

(iv)

;	1'	d	s	t
1'	1'	d	s	t
d	d	1'	t	s
s	s	t	$1' + s + t$	0'
t	t	s	0'	$1' + s + t$

(v)

;	1'	d	s	t
1'	1'	d	s	t
d	d	$1' + d + t$	$s + t$	$d + s$
s	s	$s + t$	$1' + d + s$	$d + t$
t	t	$d + s$	$d + t$	$1' + s$

3.41. Let $(A, +, -)$ be a Boolean algebra with sixteen elements and four atoms, 1', d, s, and t. Define 1' and d to be their own converses, and define the converses of s and t to be t and s respectively. If the relative multiplication table for atoms is one of the following (where $0' = d + s + t$), prove that the resulting algebra is a relation algebra.

(i)

;	1'	d	s	t
1'	1'	d	s	t
d	d	1'	t	s
s	s	t	d	1'
t	t	s	1'	d

(ii)

;	1'	d	s	t
1'	1'	d	s	t
d	d	1'	t	s
s	s	t	0'	$1' + s + t$
t	t	s	$1' + s + t$	0'

(iii)

;	1'	d	s	t
1'	1'	d	s	t
d	d	$1' + d$	$s + t$	$s + t$
s	s	$s + t$	$d + s$	1
t	t	$s + t$	1	$d + t$

(iv)

;	1'	d	s	t
1'	1'	d	s	t
d	d	$1' + s + t$	0'	0'
s	s	0'	$d + t$	$1' + d$
t	t	0'	$1' + d$	$d + s$

3.42. Prove that (R1) is independent of the remaining axioms of relation algebra.

3.43. Prove that (R2) is independent of the remaining axioms of relation algebra.

3.44. Prove that (R3) is independent of the remaining axioms of relation algebra.

3.45. Prove that (R5) is independent of the remaining axioms of relation algebra.

3.46. Prove that (R6) is independent of the remaining axioms of relation algebra.

3.47. Prove that (R7) is independent of the remaining axioms of relation algebra.

3.48. Prove that (R8) is independent of the remaining axioms of relation algebra.

3.49. Prove that (R9) is independent of the remaining axioms of relation algebra.

3.50. Prove that (R10) is independent of the remaining axioms of relation algebra.

Chapter 4
Arithmetic

The equational language of relation algebras is highly expressive, and the deductive power of the equational theory is substantial. In fact, every statement about binary relations that can be expressed in the first-order language of relations using at most three variables can equivalently be expressed as an equation in the language of relation algebras, and vice versa. Furthermore, an equation is derivable from the axioms of relation algebras if and only if a corresponding three-variable sentence is provable in a certain restricted version of first-order logic in which there are just three variables. (See either Givant [35] or Tarski-Givant [113] for details.) A consequence of these observations is that, in contrast to the arithmetic of, say, Boolean algebras, the arithmetic of relation algebras—and in particular, the study of the laws that are true in all relation algebras—is extremely complex. In fact, it is known that there is no mechanical procedure by means of which one could determine whether or not any given equation in the language of relation algebras is true in all relation algebras. In technical jargon, the equational theory of relation algebras is *undecidable*.

We shall content ourselves with a somewhat limited presentation of the arithmetic of relation algebras, enough to form a basis for the algebraic investigations in later chapters and to give readers a sense of how one can proceed in developing this arithmetic. In formulating various laws, it will always be assumed that the variables r, s, t, etc. range over the elements of an arbitrary but fixed relation algebra $\mathfrak{A}$, which will usually not be explicitly mentioned. Also, we shall often justify steps in derivations that are based upon laws of Boolean algebra by using such phrases as "by Boolean algebra".

S. Givant, *Introduction to Relation Algebras*,
DOI 10.1007/978-3-319-65235-1_4

4.1 Basic laws and duality principles

We begin with some observations that follow from the axioms concerning converse. The function φ that maps each element r in a relation algebra $\mathfrak{A}$ to its converse $r^{\smile}$ is a bijection of the universe of $\mathfrak{A}$. Indeed, if $\varphi(r) = \varphi(s)$, then $r^{\smile} = s^{\smile}$, by the definition of φ, and therefore

$$r = r^{\smile\smile} = s^{\smile\smile} = s,$$

by (R6), so φ is one-to-one. If r is any element in $\mathfrak{A}$, then

$$\varphi(r^{\smile}) = r^{\smile\smile} = r,$$

by the definition of φ and (R6), so φ is onto. This function preserves the operation of addition in the sense that

$$\varphi(r + s) = (r + s)^{\smile} = r^{\smile} + s^{\smile} = \varphi(r) + \varphi(s),$$

by (R9). The Boolean partial ordering $\leq$, and consequently also the Boolean operations of multiplication, subtraction, and symmetric difference, and the Boolean constants zero and one, are all definable in terms of addition, so they, too, must be preserved by φ. Conclusion: φ is an automorphism of the Boolean part of $\mathfrak{A}$. This leads at once to a series of easy but important laws.

Lemma 4.1. (i) $r \leq s$ *if and only if* $r^{\smile} \leq s^{\smile}$.
(ii) $(r \cdot s)^{\smile} = r^{\smile} \cdot s^{\smile}$.
(iii) $(r - s)^{\smile} = r^{\smile} - s^{\smile}$.
(iv) $(r \ominus s)^{\smile} = r^{\smile} \ominus s^{\smile}$.
(v) $(-r)^{\smile} = -(r^{\smile})$.
(vi) $r^{\smile} = 0$ *if and only if* $r = 0$, *and* $r^{\smile} = 1$ *if and only if* $r = 1$.
(vii) r *is an atom if and only if* $r^{\smile}$ *is an atom.*

The first law is called the *monotony law for converse*, and the second, third, fourth, and fifth are the *distributive laws for converse* over multiplication, subtraction, symmetric difference, and complement respectively. Since suprema and infima are also definable in terms of $\leq$, the Boolean isomorphism properties of the mapping φ imply that converse is completely distributive over addition and multiplication.

Lemma 4.2. *If the supremum or the infimum of a set* X *of elements exists, then the supremum or the infimum of the set* $\{r^{\smile} : r \in X\}$ *also exists, and*

$$\sum\{r^{\smile} : r \in X\} = (\sum X)^{\smile} \quad or \quad \prod\{r^{\smile} : r \in X\} = (\prod X)^{\smile}$$

respectively.

Converse also preserves the identity element.

Lemma 4.3. $1'^{\smile} = 1'$.

Proof. For any element r, we have $r^{\smile} ; 1' = r^{\smile}$, by (R5). Consequently,

$$r = r^{\smile\smile} = (r^{\smile} ; 1')^{\smile} = 1'^{\smile} ; r^{\smile\smile} = 1'^{\smile} ; r,$$

by (R6), the preceding observation, and (R7). This argument shows that $1'^{\smile}$ is a left-hand identity element for relative multiplication. Replace r by $1'^{\smile}$ in the equation $r ; 1' = r$, and by $1'$ in the equation $1'^{\smile} ; r = r$, to arrive at

$$1'^{\smile} = 1'^{\smile} ; 1' = 1'.$$

□

Define an operation $\odot$ on the universe of a relation algebra $\mathfrak{A}$ by

$$r \odot s = s ; r$$

for all elements r and s in $\mathfrak{A}$. The Boolean automorphism φ defined before Lemma 4.1 maps relative products to $\odot$-products in the sense that

$$\varphi(r ; s) = (r ; s)^{\smile} = s^{\smile} ; r^{\smile} = r^{\smile} \odot s^{\smile} = \varphi(r) \odot \varphi(s).$$

Also, φ preserves converse in the sense that

$$\varphi(r^{\smile}) = r^{\smile\smile} = \varphi(r)^{\smile},$$

and φ maps $1'$ to itself, by the previous lemma. Thus, φ is an *isomorphism* from the algebra $\mathfrak{A}$ to the algebra

$$\mathfrak{A}' = (A\,, +\,, -\,, \odot\,, {}^{\smile}\,, 1')$$

in the sense that φ is a bijection from the universe of $\mathfrak{A}$ to the universe of $\mathfrak{A}'$ that preserves the fundamental operations of the algebras (see Chapter 7). Consequently, $\mathfrak{A}'$ is also a relation algebra. In particular, every valid relation algebraic law continues to hold when the operation $;$ is replaced everywhere by $\odot$. We shall call this the *first duality principle* for relation algebras. The formulations and proofs of relation algebraic laws that result from this principle all have the same flavor. Here are some concrete examples.

Lemma 4.4. (i) $r\,;(s+t) = r\,;s + r\,;t$.
(ii) $1'\,;r = r$.
(iii) $-(s\,;r)\,;r^{\smile} + -s = -s$.

Proof. As an example, here is the proof of the first law:

$$r\,;(s+t) = (s+t)\odot r = s\odot r + t\odot r = r\,;s + r\,;t,$$

by the definition of $\odot$ and the fact that (R8) holds in $\mathfrak{A}'$. $\square$

The first law in the preceding lemma is the *left-hand distributive law for relative multiplication* over addition, while the second is the *left-hand identity law for relative multiplication*. We shall usually not bother to distinguish between the left-hand and right-hand versions of laws when citing those laws in derivations; for example, we shall simply say "by the distributive law for relative multiplication" or "by the identity law for relative multiplication". One can also refer to the laws formulated in (i)–(iii) as the *first duals* of (R8), (R5), and (R10) respectively. The first duality principle implies that every relation algebraic law has a first dual. For instance, in the next lemma it is shown that $r \le r\,;1$. The first dual of this law says that $r \le 1\,;r$. We shall usually not bother to formulate the first dual of laws that we prove. There are, however, a few exceptional cases when we explicitly state these duals because they are frequently used and not quite straightforward to formulate.

Lemma 4.5. (i) *If* $r \le t$ *and* $s \le u$, *then* $r\,;s \le t\,;u$.
(ii) $(r\cdot s)\,;(t\cdot u) \le (r\,;t)\cdot(s\,;u)$.
(iii) $r \le r\,;1$.
(iv) $1\,;1 = 1$.

Proof. Use the first hypothesis in (i), the definition of $\le$, and (R8) to obtain first $r+t=t$, then $r\,;s + t\,;s = t\,;s$, and finally $r\,;s \le t\,;s$. This inequality (with r, s, and t replaced by s, t, and u respectively), the second hypothesis in (i), and the first duality principle lead to inequality $t\,;s \le t\,;u$. Combine these two inequalities to arrive at the conclusion of (i).

The Boolean inequalities

$$r\cdot s \le r, \qquad r\cdot s \le s, \qquad t\cdot u \le t, \qquad t\cdot u \le u,$$

together with (i), imply that

$$(r \cdot s) \mathbin{;} (t \cdot u) \le r \mathbin{;} t \qquad \text{and} \qquad (r \cdot s) \mathbin{;} (t \cdot u) \le s \mathbin{;} u.$$

These last two inequalities and Boolean algebra lead directly to (ii).

The unit 1 is the largest element in $\mathfrak{A}$, so 1’ ≤ 1. Apply (R5) and (i) to arrive at

$$r = r \mathbin{;} 1\text{’} \le r \mathbin{;} 1.$$

Replace r by 1 in this inequality to obtain $1 \le 1 \mathbin{;} 1$. The reverse inequality follows from the fact that 1 is the largest element in $\mathfrak{A}$, so we obtain (iv). □

The implication in part (i) of the preceding lemma is called the *monotony law for relative multiplication.* It is used again and again in derivations of relation algebraic laws.

In analogy with the distributive law for relative multiplication (over addition), there is also what might be called the *semi-distributive law for relative multiplication* over subtraction.

Lemma 4.6. $(r \mathbin{;} s) - (r \mathbin{;} t) \le r \mathbin{;} (s - t)$ *and* $(r \mathbin{;} t) - (s \mathbin{;} t) \le (r - s) \mathbin{;} t$.

Proof. It suffices to derive the first law, since the first dual of this law is just the second law. From $s \cdot t \le t$, we obtain $r \mathbin{;} (s \cdot t) \le r \mathbin{;} t$, by the monotony law for relative multiplication. Forming complements reverses inequalities, so $-(r \mathbin{;} t) \le -[r \mathbin{;} (s \cdot t)]$ and therefore

$$(r \mathbin{;} s) - (r \mathbin{;} t) = (r \mathbin{;} s) \cdot -(r \mathbin{;} t) \le (r \mathbin{;} s) \cdot -[r \mathbin{;} (s \cdot t)],$$

by the definition of subtraction and Boolean algebra. Also,

$$r \mathbin{;} s = r \mathbin{;} (s - t + s \cdot t) = r \mathbin{;} (s - t) + r \mathbin{;} (s \cdot t),$$

by Boolean algebra and the distributive law for relative multiplication. Combine this with the preceding inequality, and use Boolean algebra to arrive at

$$\begin{aligned}
(r \mathbin{;} s) - (r \mathbin{;} t) &\le (r \mathbin{;} s) \cdot -[r \mathbin{;} (s \mathbin{;} t)] \\
&= [r \mathbin{;} (s - t) + r \mathbin{;} (s \cdot t)] \cdot -[r \mathbin{;} (s \cdot t)] \\
&= [r \mathbin{;} (s - t)] \cdot -[r \mathbin{;} (s \cdot t)] + [r \mathbin{;} (s \cdot t)] \cdot -[r \mathbin{;} (s \cdot t)] \\
&= [r \mathbin{;} (s - t)] \cdot -[r \mathbin{;} (s \cdot t)] + 0 \\
&\le r \mathbin{;} (s - t),
\end{aligned}$$

as desired. □

The function ψ mapping each element r in a relation algebra $\mathfrak{A}$ to its complement $-r$ is also a bijection of the universe of $\mathfrak{A}$. It maps Boolean sums to Boolean products in the sense that

$$\psi(r+s) = -(r+s) = -r \cdot -s = \psi(r) \cdot \psi(s),$$

and it maps relative products to relative sums in the sense that

$$\psi(r\,;s) = -(r\,;s) = -r \dagger -s = \psi(r) \dagger \psi(s).$$

It also preserves complements and converses in the sense that

$$\psi(-r) = -(-r) = -\psi(r) \quad \text{and} \quad \psi(r^{\smile}) = -(r^{\smile}) = (-r)^{\smile} = \psi(r)^{\smile},$$

by Lemma 4.1(v), and it interchanges 0 and 1, and 0' and 1'. It follows that ψ is an isomorphism from $\mathfrak{A}$ to the algebra

$$\mathfrak{A}'' = (A\,,\ \cdot\,,\ -\,,\ \dagger\,,\ {}^{\smile}\,,\ 0').$$

Consequently, $\mathfrak{A}''$ is a relation algebra. This implies that every valid relation algebraic law continues to hold when the operations of addition and relative multiplication are replaced everywhere by multiplication and relative addition respectively, and vice versa; and the distinguished constants 0 and 1' are replaced everywhere by 1 and 0' respectively, and vice versa. In the case of inequalities, the inequality sign must be reversed when forming a second dual. We shall call this the *second duality principle* for relation algebras. The next lemma gives some examples of laws that result from this principle.

Lemma 4.7. (i) $r \dagger (s \dagger t) = (r \dagger s) \dagger t$.
(ii) $r \dagger 0' = 0' \dagger r = r$.
(iii) $(r \dagger s)^{\smile} = s^{\smile} \dagger r^{\smile}$.
(iv) $(r \cdot s) \dagger t = (r \dagger t) \cdot (s \dagger t)$ *and* $r \dagger (s \cdot t) = (r \dagger s) \cdot (r \dagger t)$.
(v) $(r^{\smile} \dagger -(r \dagger s)) \cdot -s = -s$.
(vi) $0'^{\smile} = 0'$.
(vii) *If* $r \leq t$ *and* $s \leq u$, *then* $r \dagger s \leq t \dagger u$.
(viii) $r \dagger 0 \leq r$.
(ix) $0 \dagger 0 = 0$.

Proof. Here, as an example, is a direct derivation of (vii). If $r \leq t$ and $s \leq u$, then $-r \geq -t$ and $-s \geq -u$, by Boolean algebra, and therefore

$$-r\,;-s \geq -t\,;-u,$$

by the monotony law for relative multiplication. Form the complement of both sides of this inequality, and use Boolean algebra and the definition of relative addition, to arrive at the desired conclusion. □

The laws in (i)–(iv) and (vii) are respectively called the *associative law for relative addition*, the *identity law for relative addition*, the (*second*) *involution law for relative addition*, the *distributive law for relative addition* over multiplication, and the *monotony law for relative addition*. Alternatively, one can refer to (i)–(ix) as the *second duals* of (R4), (R5) and Lemma 4.4(ii), (R7), (R8) and Lemma 4.4(i), (R10), Lemma 4.3, and parts (i), (iii), and (iv) of Lemma 4.5 respectively. The second duality principle implies that every relation algebraic law has a second dual. We shall usually not bother to formulate these duals separately.

Define an operation $\oplus$ on the universe of a relation algebra $\mathfrak{A}$ by

$$r \oplus s = s \mathbin{+\!\!\!,} r$$

for all elements r and s in $\mathfrak{A}$. The composition of the mappings φ with ψ is an isomorphism from $\mathfrak{A}$ to the algebra

$$\mathfrak{A}''' = (A\,,\,\cdot\,,\,-\,,\,\oplus\,,\,{}^{\smile}\,,\,0\text{'}).$$

In particular, $\mathfrak{A}'''$ is a relation algebra. Consequently, if in any valid relation algebraic law we replace $+$ by $\cdot$ (and vice versa), and ; by $\oplus$ (and vice versa), and 0 by 1, and 0' by 1' (and vice versa), then we obtain another valid relation algebraic law. This is called the *third duality principle* for relation algebras. For example, the *third dual* of (R10) is

$$(-(s \mathbin{+\!\!\!,} r) \mathbin{+\!\!\!,} r^{\smile}) \cdot -s = -s.$$

This law is the first dual of Lemma 4.7(v), which in turn is the second dual of (R10).

4.2 De Morgan-Tarski laws

The next lemma shows that an abstract form of the De Morgan-Tarski laws is valid in every relation algebra. These laws are fundamental in the development of the entire arithmetic of relation algebras. As we shall see, the equivalences contained in these laws can be expressed in several different ways.

Lemma 4.8. *The following three equations are equivalent.*

(i) $(r ; s) \cdot t = 0$.
(ii) $(r^{\smile} ; t) \cdot s = 0$.
(iii) $(t ; s^{\smile}) \cdot r = 0$.

Proof. If (i) holds, then $t \leq -(r ; s)$, by Boolean algebra, and consequently

$$r^{\smile} ; t \leq r^{\smile} ; -(r ; s),$$

by the monotony law for relative multiplication. Since $r^{\smile} ; -(r ; s)$ is below $-s$, by (R10), it follows that $(r^{\smile} ; t) \leq -s$, and this last inequality is equivalent to (ii), by Boolean algebra. To establish the reverse implication, assume that (ii) holds and apply the implication from (i) to (ii) that was just proved (with $r^{\smile}$, t, and s in place of r, s, and t respectively) to obtain $(r^{\smile\smile} ; s) \cdot t = 0$. Invoke (R6) to arrive at (i).

It has been shown that (i) and (ii) are equivalent. In view of the first duality principle, this implies that

$$(s ; r) \cdot t = 0 \qquad \text{if and only if} \qquad (t ; r^{\smile}) \cdot s = 0.$$

Interchange r and s in this equivalence to arrive at the equivalence of (i) and (iii). □

The implication from (i) to (ii) in the preceding lemma is just (R11). In particular, we see that on the basis of the remaining axioms, (R10) implies (R11). It is not difficult to check that the reverse implication also holds. Indeed, put $t = -(r ; s)$ and observe that $(r ; s) \cdot t = 0$, by Boolean algebra. Assuming (R11), we obtain $(r^{\smile} ; t) \cdot s = 0$ and therefore $r^{\smile} ; t \leq -s$, that is to say,

$$r^{\smile} ; -(r ; s) \leq -s.$$

Thus, on the basis of the remaining relation algebraic axioms, (R10) is equivalent to Lemma 4.8, and in fact to the special case of the lemma contained in the implication from (i) to (ii).

The De Morgan-Tarski laws may be expressed in the following useful forms.

Corollary 4.9. *The following inequalities are equivalent.*

(i) $r ; s \leq -t$.
(ii) $r^{\smile} ; t \leq -s$.

(iii) $t\,;s^{\smile} \le -r$.
(iv) $t^{\smile}\,;r \le -(s^{\smile})$.
(v) $s\,;t^{\smile} \le -(r^{\smile})$.
(vi) $s^{\smile}\,;r^{\smile} \le -(t^{\smile})$.

Proof. The equivalence of (i)–(iii) is just the content of Lemma 4.8. The remaining equivalences are just variants of these three. For instance, if (ii) holds, then take the converse of both sides of this inequality, and apply the monotony law for converse, (R7), (R6), and Lemma 4.1(v) to arrive at (iv). □

One may view the six inequalities in the preceding corollary as involving permutations of the variables r, s, and t. From this perspective, the six inequalities cycle through the six possible permutations. For this reason, the equivalences are sometimes referred to as the *cycle laws* (see the related remark at the end of Section 2.1).

There is also a highly useful version of the De Morgan-Tarski laws that applies to atoms.

Corollary 4.10. *The following are equivalent for all atoms r, s, and t.*

(i) $t \le r\,;s$.
(ii) $s \le r^{\smile}\,;t$.
(iii) $r \le t\,;s^{\smile}$.

Proof. As an example, here is a proof of the equivalence of (i) and (ii):

$$\begin{aligned} t \le r\,;s \qquad &\text{if and only if} \qquad (r\,;s)\cdot t \neq 0,\\ &\text{if and only if} \qquad (r^{\smile}\,;t)\cdot s \neq 0,\\ &\text{if and only if} \qquad s \le r^{\smile}\,;t, \end{aligned}$$

by the assumption that t and s are atoms, and the equivalence of (i) and (ii) in Lemma 4.8. □

The inequalities contained in this corollary may be visualized (and remembered) by means of a single directed triangle, namely the triangle in Figure 4.1(a), which represents the inequality $t \le r;s$. The triangle can be rotated counterclockwise through angles of 120° and 240° to represent the other two inequalities. The bottom side of any of the rotated versions of triangle (a) is understood to be below the relative product of the other two sides, but this relative product must be formed in accordance with the direction of the arrows: both arrows

should form a path that points to the same vertex as the bottom arrow. When the side arrows are pointing in directions that do not form a path, as in (b) and (c), it is understood that the converse of one side—namely side s in (b) and side r in (c)—must be formed in order to reverse the direction of an arrow so that a proper path is formed. Thus, the second triangle represents the inequality $r \le t \,;\, s^{\smile}$, while the third represents the inequality $s \le r^{\smile} \,;\, t$.

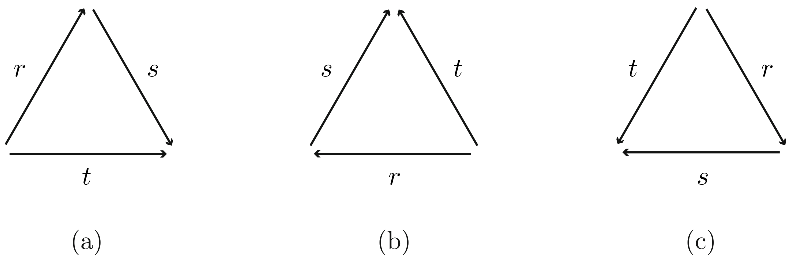


Fig. 4.1 The triangle in (a) represents the inequality $t \le r \,;\, s$, the one in (b) the inequality $r \le t \,;\, s^{\smile}$, and the one in (c) the inequality $s \le r^{\smile} \,;\, t$.

This is an appropriate moment to mention two related laws that could have been proved much earlier. The first follows from (R10) with $s = 1$.

Lemma 4.11. $r^{\smile} \,;\, -(r \,;\, 1) = 0$.

The second follows from (R10) with $s = 1$', and an application of (R5).

Lemma 4.12. $r^{\smile} \,;\, -r \le 0$'.

It can be shown that, on the basis of (R1)–(R9), the laws in the preceding two lemmas are jointly equivalent to (R10) and hence to the De Morgan-Tarski laws. The proof is left as an exercise.

It is always informative to examine the logical meaning of a relation algebraic law. For example, Lemma 4.12 says, in the context of set relation algebras, that

$$R^{-1} \,|\, {\sim}R \subseteq di_U$$

for every relation R on a set U. By applying the definitions of the operations and the distinguished relation involved in this inclusion, we see that the logical meaning of the inclusion can be formulated as follows: given elements α and β, if there is a γ such that the pair (γ, α)

belongs to a relation R, and the pair (γ, β) does not belong to R, then we must have $\alpha \neq \beta$.

The second dual of Lemma 4.12 is used quite often, so it is helpful to formulate it explicitly.

Corollary 4.13. $1' \leq r^{\smile} \mathbin{+\!\!\!,}\, -r$.

4.3 Definability of converse

It was pointed out earlier that the Boolean operations and Boolean distinguished constants are all definable in terms of addition alone. It is natural to inquire whether the Peircean operations and distinguished constants are definable in terms of relative multiplication, perhaps with the help of addition. This turns out, in fact, to be the case. Clearly, the identity element is definable in terms of relative multiplication alone, since

$$t = 1' \quad \text{if and only if} \quad r \,;t = t\,;r = r \quad \text{for every } r.$$

The next lemma shows that converse is definable in terms of relative multiplication, the diversity element, and the Boolean operations. Since the diversity element is definable in terms of the identity element, which in turn is definable in terms of relative multiplication, and since the Boolean operations are definable in terms of addition, it follows that converse is definable in terms of relative multiplication and addition. Consequently, all of the Peircean operations and distinguished constants are definable in terms of relative multiplication and addition.

Lemma 4.14. $r^{\smile}$ *is the largest element* s *such that* $s\,; -r \leq 0'$.

Proof. Certainly, the element $r^{\smile}$ satisfies the inequality

$$s\,; -r \leq 0', \tag{1}$$

by Lemma 4.12. It remains to show that any element s satisfying (1) must be below $r^{\smile}$. The inequality in (1) implies that $(s\,; -r) \cdot 1' = 0$, and therefore $(s^{\smile}\,; 1') \cdot -r = 0$, by the implication from (i) to (ii) in Lemma 4.8. Apply the identity law to arrive at $s^{\smile} \cdot -r = 0$, and therefore $s^{\smile} \leq r$. Form the converse of both sides of this last inequality, and apply the monotony law for converse and the first involution law, to conclude that $s \leq r^{\smile}$. □

The form of the preceding definition implicitly involves a logical implication, and therefore a logical negation. It says, in essence, that $t = r^{\smile}$ if and only if

$$t\,;-r + 0' = 0', \text{ and for all } s, \text{ if } s\,;-r + 0' = 0', \text{ then } s + t = t.$$

Interestingly, converse can also be defined by a positive formula, that is to say, by a formula that does not explicitly or implicitly involve logical negation.

Lemma 4.15. *$t = r^{\smile}$ if and only if*

$$t\,;-r + 0' = 0' \qquad \textit{and} \qquad r\,;-t + 0' = 0'.$$

Proof. If $t = r^{\smile}$, then $r = t^{\smile}$, by the first involution law, and therefore the two equations on the right side of the equivalence hold, by two applications of Lemma 4.12 (the first by writing t in place of $r^{\smile}$, and the second by replacing r everywhere with t and then writing r in place of $t^{\smile}$). On the other hand, if t satisfies the two equations on the right side of the equivalence, then $t \le r^{\smile}$ and $r \le t^{\smile}$, by two applications of Lemma 4.14 (the first with s replaced by t, and the second with r and s replaced by t and r respectively). It follows that $t \le r^{\smile}$ and $r^{\smile} \le t$, by the monotony law for relative multiplication and the first involution law, so $t = r^{\smile}$. □

4.4 Consequences of the De Morgan-Tarski laws

The De Morgan-Tarski laws are rich in consequences. They imply, for example, that relative multiplication is completely distributive.

Lemma 4.16. *If the sum of a set X of elements exists, then the sums of the sets $\{r\,;s : s \in X\}$ and $\{s\,;r : s \in X\}$ also exist, and*

$$\sum\{r\,;s : s \in X\} = r\,;(\sum X) \quad \textit{and} \quad \sum\{s\,;r : s \in X\} = (\sum X)\,;r.$$

Proof. It suffices to establish the first equality, by the first duality principle. Write

$$t = \sum X \qquad \text{and} \qquad Y = \{r\,;s : s \in X\}.$$

For each element s in X, we have $s \le t$, and therefore $r\,;s \le r\,;t$, by the monotony law for relative multiplication. Consequently, $r\,;t$ is an

upper bound of the set Y. Let u be any upper bound of Y. For each element s in X, the product $r\,;s$ is below u, by assumption and the definition of Y, so

$$(r\,;s)\cdot -u = 0.$$

Apply Lemma 4.8 to obtain $(r^{\smile}\,;-u)\cdot s = 0$. This last equation is true for every s in X, so

$$\begin{aligned}(r^{\smile}\,;-u)\cdot t &= (r^{\smile}\,;-u)\cdot (\textstyle\sum X)\\ &= \textstyle\sum\{(r^{\smile}\,;-u)\cdot s : s \in X\} = 0, \qquad (1)\end{aligned}$$

by the definition of t and the completely distributivity of multiplication. Apply Lemma 4.8 to (1) to arrive at $(r\,;t)\cdot -u = 0$, or equivalently, $r\,;t \leq u$. Thus, $r\,;t$ is the least upper bound of Y. □

Take the set X to be empty in the preceding lemma to obtain the following corollary, which—together with its first dual—asserts that relative multiplication is a normal operation (see Section 2.2).

Corollary 4.17. $r\,;0 = 0$.

The complete distributivity of relative multiplication is very often applied in the following equivalent form (see Lemma 2.4).

Corollary 4.18. *If the suprema of two sets of elements X and Y exist, then the supremum of the set $\{r\,;s : s \in X$ and $s \in Y\}$ exists, and*

$$\textstyle\sum\{r\,;s : s \in X \textit{ and } s \in Y\} = (\sum X)\,;(\sum Y).$$

The next law is among the most important in the theory of relation algebras. It and its first dual are used again and again in more sophisticated derivations.

Lemma 4.19. $(r\,;s)\cdot t \leq r\,;[s\cdot(r^{\smile}\,;t)]$.

Proof. Apply the implication from (ii) to (i) in Corollary 4.9 (with s replaced by $s\cdot -(r^{\smile}\,;t)$) to the obvious inequality

$$r^{\smile}\,;t \leq -s + r^{\smile}\,;t = -[s\cdot -(r^{\smile}\,;t)]$$

to obtain

$$r\,;[s\cdot -(r^{\smile}\,;t)] \leq -t. \qquad (1)$$

The monotony law for relative multiplication implies that

$$r\,;[s\cdot -(r^{\smile}\,;t)]\le r\,;s.$$

Combine this inequality with (1), and use Boolean algebra, to obtain

$$r\,;[s\cdot -(r^{\smile}\,;t)]\le (r\,;s)\cdot -t. \tag{2}$$

Add $r\,;[s\cdot (r^{\smile}\,;t)]$ to both sides of (2) to arrive at

$$r\,;[s\cdot -(r^{\smile}\,;t)] + r\,;[s\cdot (r^{\smile}\,;t)] \le (r\,;s)\cdot -t + r\,;[s\cdot (r^{\smile}\,;t)]. \tag{3}$$

Since

$$\begin{aligned} r\,;[s\cdot -(r^{\smile}\,;t)] + r\,;[s\cdot (r^{\smile}\,;t)] &= r\,;[s\cdot -(r^{\smile}\,;t) + s\cdot (r^{\smile}\,;t)] \\ &= r\,;[s\cdot (-(r^{\smile}\,;t) + (r^{\smile}\,;t))] = r\,;(s\cdot 1) = r\,;s, \end{aligned}$$

by the distributive law for relative multiplication and Boolean algebra, it follows from (3) that

$$r\,;s\le (r\,;s)\cdot -t + r\,;[s\cdot (r^{\smile}\,;t)].$$

Form the product of both sides of this inequality with t, and use Boolean algebra, to conclude that

$$\begin{aligned} (r\,;s)\cdot t &\le ((r\,;s)\cdot -t + r\,;[s\cdot (r^{\smile}\,;t)])\cdot t \\ &= (r\,;s)\cdot -t\cdot t + (r\,;[s\cdot (r^{\smile}\,;t)])\cdot t \\ &= (r\,;[s\cdot (r^{\smile}\,;t)])\cdot t \le r\,;[s\cdot (r^{\smile}\,;t)], \end{aligned}$$

as desired. □

The first dual of Lemma 4.19 is used often enough to warrant its explicit formulation.

Corollary 4.20. $(r\,;s)\cdot t\le [(t\,;s^{\smile})\cdot r]\,;s$.

The derivations of the laws in the next seven corollaries and lemmas all depend on Lemma 4.19.

Corollary 4.21. $(r\,;s)\cdot t\le r\,;r^{\smile}\,;t$.

Proof. We have

$$(r\,;s)\cdot t\le r\,;[s\cdot (r^{\smile}\,;t)]\le r\,;r^{\smile}\,;t,$$

by Lemma 4.19 and the monotony law for relative multiplication. □

Corollary 4.22. $r \leq r\,;r^{\smile}\,;r$.

Proof. Take s and t in Corollary 4.21 to be 1' and r respectively, and use also the identity law for relative multiplication, to obtain

$$r = (r\,;1')\cdot r \leq r\,;r^{\smile}\,;r,$$

as desired. □

By taking $r \cdot s \cdot t$ for r in the preceding corollary, and then using Lemma 4.1(ii) and the monotony law for relative multiplication, we obtain the following rather interesting consequence of the previous corollary.

Corollary 4.23. $r \cdot s \cdot t \leq r\,;s^{\smile}\,;t$.

This corollary implies a kind of Boolean analogue of Lemma 4.12.

Lemma 4.24. $r^{\smile} \cdot -r \leq 0'$.

Proof. Apply Corollary 4.23 (with r, s, and t replaced by $r^{\smile}$, 1', and $-r$ respectively), Lemma 4.3, (R5), and Lemma 4.12 to obtain

$$r^{\smile} \cdot 1' \cdot -r \leq r^{\smile}\,;1'^{\smile}\,;-r = r^{\smile}\,;1'\,;-r = r^{\smile}\,;-r \leq 0'.$$

Every element below 1' is disjoint from 0', so the preceding inequality implies that $(r^{\smile} \cdot -r) \cdot 1' = 0$ and therefore $r^{\smile} \cdot -r \leq 0'$. □

There is a sharper form of Lemma 4.19 that essentially combines the inequalities of the lemma and its first dual into one law.

Lemma 4.25. $(r\,;s)\cdot t \leq [(t\,;s^{\smile})\cdot r]\,;[s\cdot(r^{\smile}\,;t)]$.

Proof. Corollary 4.20 and Boolean algebra yield

$$(r\,;s)\cdot t \leq [(t\,;s^{\smile})\cdot r]\,;s \qquad \text{and} \qquad (r\,;s)\cdot t \leq t$$

respectively, from which it follows that

$$(r\,;s)\cdot t \leq ([(t\,;s^{\smile})\cdot r]\,;s)\cdot t. \tag{1}$$

Use Lemma 4.19 (with $(t\,;s^{\smile})\cdot r$ in place of r) to obtain

$$([(t\,;s^{\smile})\cdot r]\,;s)\cdot t \leq [(t\,;s^{\smile})\cdot r]\,;[s\cdot([(t\,;s^{\smile})\cdot r]^{\smile}\,;t)]. \tag{2}$$

Since $[(t\,;s^{\smile})\cdot r]^{\smile}$ is below $r^{\smile}$, by the monotony law for converse, the inequality in (2) implies that

$$([(t\,;s^{\smile})\cdot r]\,;s)\cdot t \leq [(t\,;s^{\smile})\cdot r]\,;[s\cdot(r^{\smile}\,;t)]. \tag{3}$$

Combine (1) and (2) to arrive at the desired conclusion. □

Both Lemma 4.19 and Corollary 4.20 follow from the preceding lemma by simple applications of the monotony law for relative multiplication.

Lemma 4.26. $r\,;1\,;s = (r\,;1)\cdot(1\,;s)$.

Proof. The monotony law for relative multiplication implies that

$$r\,;1\,;s \le r\,;1 \qquad \text{and} \qquad r\,;1\,;s \le 1\,;s,$$

so $r\,;1\,;s$ is below the product $(r\,;1)\cdot(1\,;s)$. For the reverse inequality, we have

$$(r\,;1)\cdot(1\,;s) \le r\,;(1\cdot[r^{\smile}\,;(1\,;s)]) = r\,;(r^{\smile}\,;1\,;s) \le r\,;1\,;s,$$

by Lemma 4.19 (with 1 and $1\,;s$ in place of s and t), Boolean algebra, and the monotony law for relative multiplication. □

The next law is of interest because of its close similarity in form to an inequality we shall encounter later that is true in all set relation algebras but that is not derivable from the axioms of relation algebra (see Section 17.5).

Lemma 4.27. $(r\,;s)\cdot(t\,;u) \le r\,;[(r^{\smile}\,;t)\cdot(s\,;u^{\smile})]\,;u$.

Proof. Use Lemma 4.19 (with t replaced by $t\,;u$), (R4), and Boolean algebra to obtain

$$(r\,;s)\cdot(t\,;u) \le r\,;(s\cdot[r^{\smile}\,;(t\,;u)]) = r\,;([(r^{\smile}\,;t)\,;u]\cdot s). \tag{1}$$

Use Corollary 4.20 (with r, s, and t replaced by $r^{\smile}\,;t$, u, and s respectively) and Boolean algebra to obtain

$$[(r^{\smile}\,;t)\,;u]\cdot s \le [(s\,;u^{\smile})\cdot(r^{\smile}\,;t)]\,;u = [(r^{\smile}\,;t)\cdot(s\,;u^{\smile})]\,;u. \tag{2}$$

Combine (1) and (2), and apply the monotony law for relative multiplication, to arrive at

$$(r\,;s)\cdot(t\,;u) \le r\,;([(r^{\smile}\,;t)\,;u]\cdot s) \le r\,;[(r^{\smile}\,;t)\cdot(s\,;u^{\smile})]\,;u,$$

as desired. □

A *modular law* is a law with one of the forms

$$r \odot (s \oplus t) = (r \odot s) \oplus t \qquad \text{or} \qquad (t \oplus s) \odot r = t \oplus (s \odot r),$$

where $\oplus$ and $\odot$ are binary operations on a set. We have already encountered an example of such a law, namely the modular law for lattices, say, in the form in which the operations $\oplus$ and $\odot$ are the lattice operations of join and meet respectively (see Section 3.7). For lattices, the modular law (in the form alluded to above) requires the special hypothesis that t be included in r. This hypothesis may be avoided by replacing each occurrence of the variable t by $r \odot t$ or by $t \odot r$ respectively, so that the laws assume the forms

$$r \odot [s \oplus (r \odot t)] = (r \odot s) \oplus (r \odot t)$$

and

$$[(t \odot r) \oplus s] \odot r = (t \odot r) \oplus (s \odot r)$$

respectively. To distinguish between these forms, laws of the first two forms above are sometimes called *strong* modular laws, and laws of the second two forms are sometimes called *standard* modular laws. Usually, however, we shall simply speak of modular laws, without using the adjectives "strong" or "standard".

The following law may be viewed as a kind of *semi-modular law* for relative multiplication over relative addition.

Lemma 4.28. $(r \mathbin{+\!\!\!\!\!,\,} s) \mathbin{;} t \leq r \mathbin{+\!\!\!\!\!,\,} s \mathbin{;} t$.

Proof. Lemma 4.4(iii) (with r replaced by t) and Boolean algebra imply that

$$-(s \mathbin{;} t) \mathbin{;} t^{\smile} \leq -s.$$

Form the relative product of both sides of this inequality with $-r$ on the left, and use the associative and monotony laws for relative multiplication, the definition of relative addition, and Boolean algebra to obtain

$$[-r \mathbin{;} -(s \mathbin{;} t)] \mathbin{;} t^{\smile} = -r \mathbin{;} [-(s \mathbin{;} t) \mathbin{;} t^{\smile}] \leq -r \mathbin{;} -s = -(r \mathbin{+\!\!\!\!\!,\,} s). \tag{1}$$

Apply Corollary 4.9 (the implication from (iii) to (i), with r, s, and t replaced by $r \mathbin{+\!\!\!\!\!,\,} s$, t, and $-r \mathbin{;} -(s \mathbin{;} t)$ respectively) to (1) to arrive at

$$(r \mathbin{+\!\!\!\!\!,\,} s) \mathbin{;} t \leq -[-r \mathbin{;} -(s \mathbin{;} t)].$$

Another application of the definition of relative addition leads directly to the desired conclusion. □

It is worthwhile to formulate explicitly the first dual of Lemma 4.28.

Corollary 4.29. $r\,;(s \dagger t) \le r\,;s \dagger t$.

To understand the logical content of the semi-modular law in Lemma 4.28, we look at the law in the context of set relation algebras. Consider relations R, S, and T on a set U. A pair (α, β) of elements from U belongs to the relation $(R \dagger S) \mid T$ just in case there is an element γ in U such that for all δ in U,

$$[(\alpha, \delta) \in R \text{ or } (\delta, \gamma) \in S] \text{ and } (\gamma, \beta) \in T.$$

The pair (α, β) belongs to the relation $R \dagger (S \mid T)$ just in case for every element δ in U there is a γ in U such that

$$(\alpha, \delta) \in R \text{ or } [(\delta, \gamma) \in S \text{ and } (\gamma, \beta) \in T].$$

The inclusion

$$(R \dagger S) \mid T \subseteq R \dagger (S \mid T)$$

therefore expresses a law about reversing the order of an existential and a universal quantifier: it says that a certain $\exists\forall$ statement implies a closely related $\forall\exists$ statement. A well-known example of this type of reversing of the order of an existential and a universal quantifier occurs in the assertion that uniform continuity implies continuity.

Corollary 4.30. $(r \dagger s^{\smile})\,; -s \le r$ *and* $r \le r\,; s^{\smile} \dagger -s$.

Proof. To prove the first inequality, observe that

$$(r \dagger s^{\smile})\,; -s \le r \dagger s^{\smile}\,; -s \le r \dagger 0' = r,$$

by Lemmas 4.28 and 4.12, and the identity law for relative addition. The second inequality is the second dual of the first inequality. □

Corollary 4.31. $(r \dagger 0)\,; 1 = r \dagger 0$ *and* $r\,; 1 \dagger 0 = r\,; 1$.

Proof. We have

$$r \dagger 0 \le (r \dagger 0)\,; 1 \le r \dagger 0\,; 1 = r \dagger 0,$$

by Lemma 4.5(iii), Lemma 4.28, and the first dual of Corollary 4.17. Since the first and last terms are the same, equality must hold everywhere. This establishes the first law. The second law is just the second dual of the first law. □

We now turn to an important modular law for multiplication over relative multiplication, a law that requires certain hypotheses for its validity.

Lemma 4.32. *If* $r\,;t \le r$ *and* $-r\,;t \le -r$*, then* $r \cdot (s\,;t) = (r \cdot s)\,;t$*.*

Proof. Use Boolean algebra, Lemma 4.5(ii), and the first hypothesis to obtain

$$(r \cdot s)\,;t = (r \cdot s)\,;(t \cdot t) \le (r\,;t) \cdot (s\,;t) \le r \cdot (s\,;t). \tag{1}$$

To establish the reverse inequality, use the Boolean law $s \le r \cdot s + -r$, the monotony and distributive laws for relative multiplication, and the second hypothesis to obtain

$$s\,;t \le (r \cdot s + -r)\,;t = (r \cdot s)\,;t + -r\,;t \le (r \cdot s)\,;t + -r. \tag{2}$$

Form the product of the first and last terms in (2) with r, and use Boolean algebra, to arrive at

$$\begin{aligned} r \cdot (s\,;t) \le r \cdot [(r \cdot s)\,;t + -r] &= r \cdot [(r \cdot s)\,;t] + r \cdot -r \\ &= r \cdot [(r \cdot s)\,;t] + 0 \le (r \cdot s)\,;t. \end{aligned} \tag{3}$$

Together, (1) and (3) yield the desired conclusion. □

The preceding modular law can be written in a somewhat different form that is quite useful.

Corollary 4.33. *If* $r\,;t \le r$ *and* $r\,;t^{\smile} \le r$*, then* $r \cdot (s\,;t) = (r \cdot s)\,;t$*.*

Proof. The equations

$$(-r\,;t) \cdot r = 0 \qquad \text{and} \qquad (r\,;t^{\smile}) \cdot -r = 0$$

are equivalent, by the De Morgan-Tarski laws, so the inequalities

$$-r\,;t \le -r \qquad \text{and} \qquad r\,;t^{\smile} \le r$$

are equivalent. The corollary now follows at once from the hypotheses and Lemma 4.32. □

We saw in the brief discussion of minimal set relation algebras in Section 3.1 that the value of the relative product 0’ ; 0’ can play an important role in the structural analysis of relation algebras. This value is not uniquely determined and depends essentially on the relation algebra under discussion. (We shall have more to say about this matter in Chapter 13.) It is an interesting and rather surprising fact that a uniform value for 0’ ; 0’ ; 0’ ; 0’ can be given.

Lemma 4.34. $0' ; 0' ; 0' ; 0' = 0' ; 0'$.

Proof. The identity law for relative addition implies that

$$0' ; 0' = 0' ; 0' \mathbin{\underset{,}{+}} 0'.$$

Form the relative product of both sides of this equation with $0'$ on the right, and apply the semi-modular law in Lemma 4.28 (with r, s, and t replaced by $0' ; 0'$, $0'$, and $0'$ respectively), to obtain

$$0' ; 0' ; 0' = (0' ; 0' \mathbin{\underset{,}{+}} 0') ; 0' \leq 0' ; 0' \mathbin{\underset{,}{+}} 0' ; 0'. \tag{1}$$

Similarly,

$$0' ; 0' ; 0' = 0' ; 0' ; 0' \mathbin{\underset{,}{+}} 0',$$

by the identity law for relative addition. Form the relative product of both sides of this equation with $0'$ on the right, and apply Lemma 4.28 (with r, s, and t replaced by $0';0';0'$, $0'$, and $0'$ respectively), to obtain

$$0' ; 0' ; 0' ; 0' = (0' ; 0' ; 0' \mathbin{\underset{,}{+}} 0') ; 0' \leq 0' ; 0' ; 0' \mathbin{\underset{,}{+}} 0' ; 0'. \tag{2}$$

Combine (1) and (2), and use the monotony law for relative addition, to arrive at

$$0' ; 0' ; 0' ; 0' \leq 0' ; 0' \mathbin{\underset{,}{+}} 0' ; 0' \mathbin{\underset{,}{+}} 0' ; 0'. \tag{3}$$

Observe that

$$(0' ; 0')^{\smile} = 0'^{\smile} ; 0'^{\smile} = 0' ; 0', \tag{4}$$

by the second involution law and Lemma 4.7(vi). Apply this observation and the second dual of Corollary 4.22 (with r replaced by $0' ; 0'$) to obtain

$$0' ; 0' \mathbin{\underset{,}{+}} 0' ; 0' \mathbin{\underset{,}{+}} 0' ; 0' = 0' ; 0' \mathbin{\underset{,}{+}} (0' ; 0')^{\smile} \mathbin{\underset{,}{+}} 0' ; 0' \leq 0' ; 0'. \tag{5}$$

Combine (3) and (5) to conclude that

$$0' ; 0' ; 0' ; 0' \leq 0' ; 0'. \tag{6}$$

To establish the reverse inequality, observe that

$$\begin{aligned} 0' ; 0' &\leq 0' ; 0' ; (0' ; 0')^{\smile} ; 0' ; 0' \\ &= 0' ; 0' ; 0' ; 0' ; 0' ; 0' \leq 0' ; 0' ; 0' ; 0', \end{aligned}$$

by Corollary 4.22 (with r replaced by $0' ; 0'$), (4), and (6). □

4.5 Historical remarks

The original notations for the operations and distinguished elements of the calculus of relations were developed and modified by Peirce over a substantial period of time, as he gained insights into the subject. The final versions of his notations that were employed by him in [88] are rather different from the notations that are employed today. There, he used the symbols 0, ∞, 1, and $\mathfrak{n}$ to denote zero, one, the identity element, and the diversity element respectively; he wrote the Boolean and relative sums of two elements r and s as $r+s$ and $r \dagger s$ respectively; and he wrote the Boolean and relative products of r and s as r, s and rs respectively. The complement and the converse of an element r were rendered as $\bar{r}$ and $\breve{r}$.

The notations that are used in this book (and that were used by Tarski in his seminars on relation algebras and in [23]) are essentially due to Schröder [98], and they visibly convey the close analogy between the Boolean and Peircean notions. In fact, to obtain the symbol for each Peircean operation and constant, Schröder uses the symbol for the corresponding Boolean operation and constant, and adjoins to this symbol a comma: in the case of operations, the comma appears below the Boolean operation, and in the case of distinguished constants, it appears to the right of the Boolean constant as an apostrophe. For example, Boolean addition and multiplication are denoted in [98] by the symbols $+$ and $\cdot$, and Peircean addition and multiplication are denoted by the symbols $\underset{,}{+}$ and $;$. (Actually, a slightly modified version of $\underset{,}{+}$ is used in [98] for typographical reasons.) Similarly, the Boolean constants zero and one are denoted in [98] by the symbols 0 and 1, while the corresponding Peircean constants—the identity and diversity elements—are denoted by the symbols 1' and 0'. The only exception to this rule is the symbol $\smile$ for converse, which is not obtained by adjoining some sort of comma to the complement symbol $-$. The reason for this exception is that the Peircean counterpart of complement is not converse, but rather converse-complement, which is the unary operation ${}^{-,}$ defined by

$$r^{-,} = -(r^{\smile}).$$

Tarski deviated from Schröder's notation in one point: he did not place the symbols for complement and converse directly above variables as Schröder and Peirce did, but rather to the right of the vari-

ables, as superscripts, in order to facilitate writing more complex expressions. We have followed this deviation, but have opted to place complement symbols in front of (that is to say, to the left of) variables in order to stress the relationship of this notation to the traditional notation for negative numbers and for subtraction; in so doing, we are also staying quite close to Boole's original notation. Following Tarski, converse symbols are placed to the right of variables as superscripts in order to stress the relationship of this notation to the traditional notation for function inverses.

It was mentioned above that Schröder's notations convey visually a close analogy between Boolean and Peircean notions. In fact, every law of relation algebras becomes a valid law of Boolean algebra when the Peircean notions are replaced by their Boolean counterparts. This is just an arithmetic manifestation of the fact that every Boolean algebra can be turned into a relation algebra in a trivial way—see Section 3.4. In the reverse direction, it is not true that a Boolean law always becomes a law of relation algebras when the Boolean notions are replaced by their Peircean counterparts, but Boolean laws often do suggest Peircean analogues. For example, corresponding to the Boolean laws

$$r + -r = 1 \qquad \text{and} \qquad r \cdot -r = 0$$

are the Peircean laws

$$r \mathbin{+\!\!\!\!,}\; r^{-\smile} \geq 1' \qquad \text{and} \qquad r \,;\, r^{-\smile} \leq 0',$$

that is to say, the laws

$$r \mathbin{+\!\!\!\!,}\; (-r)^{\smile} \geq 1' \qquad \text{and} \qquad r \,;\, (-r)^{\smile} \leq 0',$$

that are valid the theory of relation algebras, by Lemma 4.12 and its second dual in Corollary 4.13 (with $r^{\smile}$ in place of r).

Peirce was certainly aware of the various duality principles that apply to laws in the calculus of relations, and Schröder explicitly mentions these principles. Many of the laws presented in this chapter may already be found in Peirce's papers. In particular, the associative laws for relative addition and multiplication, the distributive laws for relative multiplication over addition, and for relative addition over multiplication, the distributive laws for converse over addition and multiplication, the first involution law, the second involution law and its second

dual, the identity laws for relative addition and relative multiplication, Corollary 4.17 and its various duals, Lemma 4.12 and its second dual in Corollary 4.13, the semi-modular law in Lemma 4.28 and its first dual in Corollary 4.29, and the analogues for relative addition and multiplication of De Morgan's laws—that is to say, the definitions of relative addition in terms of relative multiplication and vice versa—are all explicitly mentioned in Peirce [88].

Schröder [98] contains a wealth—one might almost say an overabundance—of laws, including all those studied by Peirce. For example, one can find versions of almost all of the laws presented in Sections 4.1, 4.2, and 4.4 above, up to Corollary 4.18, and the laws in Lemmas 4.24, 4.26, and 4.28, in Corollaries 4.30 and 4.31, and in Exercises 4.14–4.24, together with all of the various duals of these laws. In particular, in place of the 6 equivalences stated in Corollary 4.9, Schröder essentially gives some 24 equivalent inequalities under the name of the first Inversion Theorem. He notes the cyclical "exchangeability" of the three variables in these inequalities, and he states that the equivalence of the first two inequalities (parts (i) and (v) of Corollary 4.9, but with t and $t^{\smile}$ interchanged) already implies all of the other equivalences.

What distinguishes Tarski's presentation of the laws of the calculus of relations from those of his predecessors is, first, its axiomatic approach and the purity of its methods of proof, and second, its focused economy. Schröder employs a variety of methods to prove laws, but very often he uses arguments that refer to individual elements, and in particular to pairs of elements belonging to relations; examples of such arguments are given in Section 1.3 above. Tarski criticizes this approach—see the relevant quote in Section 2.6—and develops the calculus of relations as an equational theory based on simple laws, without using any sentential connectives, quantifiers, or variables ranging over individuals (see [104], [105], [106], [23], and [55]). The only rules of inference that he employs are those appropriate for equational derivations.

The presentation in this chapter is inspired by the presentations in [23] and in the lecture notes from Tarski's 1970 seminar on relation algebras (see [112]). The results in Section 4.3 concerning the definability of converse in terms of addition and relative multiplication are due to Tarski: Lemma 4.14 is contained in [23], and Lemma 4.15 is presented in the 1970 seminar notes [112]. Most of the remaining results not referred to in the remarks above are explicitly stated and proved in [23], and date back to Tarski's seminars from the period

1942–45 (see [105]). They include: first, Lemma 4.19 and its consequences, Corollary 4.22 through Lemma 4.24 and Lemma 4.27; second, Corollary 4.33, which was suggested to Tarski by Jónsson, and Lemma 4.32, which was formulated and proved by Tarski in order to derive Corollary 4.33; third, Lemma 4.34, which is due to Julia Robinson; fourth, the axiomatic characterization of relation algebras in Exercise 4.26, which is due to Tarski, and the one in Exercise 4.28, which was suggested to Tarski by Hugo Ribeiro in 1947. The laws in Lemmas 4.25 and 4.26, and in Exercise 4.12 are also due to Tarski and date back to the 1942–45 seminars (see [105]), but they do not occur in [23]. Lemma 4.25 is also stated in Riguet [90] as a law about binary relations. The laws in Exercise 4.29 and the alternative proof of Lemma 4.14 implicit in Exercise 4.30 are from the 1970 seminar. The central role played by Lemma 4.8 in an axiomatic development of the calculus of relations was clearly recognized by Tarski, and it is for this reason that we have referred to the equivalences in the lemma as the De Morgan-Tarski laws.

The alternative axiomatization of the theory of relation algebras presented in Exercise 4.27 is an improvement due to Givant of a result that originates with Kamel [58] (see also Kamel [57]). Kamel's axiomatization includes (R7) as well, and Givant showed that this axiom is not needed.

Exercises

4.1. Prove the laws in Lemma 4.1 by giving explicit derivations, without using the fact that the function mapping each element to its converse is a Boolean automorphism.

4.2. Prove the laws in Lemma 4.2 by giving explicit derivations, without using the fact that the function mapping each element to its converse is a Boolean automorphism.

4.3. Prove the laws in Lemma 4.4 by giving explicit derivations, without using the first duality principle.

4.4. Formulate the first dual of Axiom (R7). What do you notice?

4.5. Prove the laws in Lemma 4.7 by giving explicit derivations, without using the second duality principle.

4.6. Derive the law

$$(1 ; r ; 1) \cdot s \neq 0 \qquad \text{if and only if} \qquad (1 ; s ; 1) \cdot r \neq 0.$$

Hint.

$$\begin{aligned} (1 ; r ; 1) \cdot s \neq 0 \qquad & \text{if and only if} \qquad (1 ; r) \cdot (s ; 1^{\smile}) \neq 0, \\ & \text{if and only if} \qquad (1 ; r) \cdot (s ; 1) \neq 0, \\ & \text{if and only if} \qquad (1^{\smile} ; s ; 1) \cdot r \neq 0, \\ & \text{if and only if} \qquad (1 ; s ; 1) \cdot r \neq 0. \end{aligned}$$

The first equivalence uses the equivalence of (i) and (iii) in Lemma 4.8 (with $1 ; r$, 1, and s in place of r, s, and t respectively), the second and fourth equivalences use Lemma 4.1(vi), and the third equivalence uses the equivalence of (i) and (ii) in Lemma 4.8 (with 1, r, and $s ; 1$ in place of r, s, and t respectively).

4.7. Complete the proof of Corollary 4.9.

4.8. Derive the law $r ; 0 = 0$ without using Lemma 4.16.

4.9. Formulate the first, second and third duals of the following laws.

(i) $r ; 0 = 0$.
(ii) $r^{\smile} ; -r \leq 0'$.

4.10. Formulate the second and third duals of the law in Lemma 4.19.

4.11. Derive Lemma 4.19 and Corollary 4.20 directly from Lemma 4.25

4.12. Derive the law $r ; [s - (r^{\smile} ; t)] \leq (r ; s) - t$.

4.13. Formulate the second dual of the law in Lemma 4.28. What do you notice?

4.14. Derive the law $1 ; [(r ; s) \cdot t] = 1 ; [(r^{\smile} ; t) \cdot s]$.

4.15. Derive the law $1 ; r ; 1 = 1 ; r^{\smile} ; 1$.

4.16. Derive the laws

$$r ; [(-r)^{\smile} \mathbin{\dagger} s] \leq s \qquad \text{and} \qquad s \leq r \mathbin{\dagger} [(-r)^{\smile} ; s].$$

4.17. Derive the laws

$$(0 \mathbin{\dagger} -r) ; r^{\smile} = 0 \qquad \text{and} \qquad (1 ; -r) \mathbin{\dagger} r^{\smile} = 1.$$

4.18. Derive the laws

$$(r\,;1)\cdot s \le r\,;r^{\smile}\,;s \qquad \text{and} \qquad r\cdot(1\,;s) \le r\,;s^{\smile}\,;s.$$

These laws are immediate consequences of Lemma 4.19 (with s and t replaced by 1 and s respectively) and Corollary 4.20 (with r and t replaced by 1 and r respectively).

4.19. Derive the law $[r\cdot(1\,;s)]\,;1 = r\,;s^{\smile}\,;1$. What is the logical meaning of this law?

4.20. Derive the law $r\,;1\,;r\,;1 = r\,;1$.

4.21. Derive the law $[(r \mathbin{\underset{,}{+}} 0)\cdot s]\,;t = (r \mathbin{\underset{,}{+}} 0)\cdot(s\,;t)$. What is the logical meaning of this law?

4.22. Derive the law $(r \mathbin{\underset{,}{+}} 0)\,;(r \mathbin{\underset{,}{+}} 0) = r \mathbin{\underset{,}{+}} 0$.

4.23. Derive the laws

$$(r \mathbin{\underset{,}{+}} 0)\cdot(1\,;s) = (r \mathbin{\underset{,}{+}} 0)\,;s \quad \text{and} \quad (r \mathbin{\underset{,}{+}} 0)+(1\,;s) = r \mathbin{\underset{,}{+}} (1\,;s).$$

4.24. Derive the law $r\,;1 \mathbin{\underset{,}{+}} 1\,;s = r\,;1+1\,;s$.

4.25. Prove that in a relation algebra, 1' is the unique element s that satisfies the equation $s\,;r = r$ for all r. This observation shows that 1' is definable in terms of relative multiplication by a positive formula.

4.26. Show that $\mathfrak{A} = (A\,,+\,,-\,,;\,,{}^{\smile}\,,1')$ is a relation algebra if and only if (R1)–(R5) and the De Morgan-Tarski laws from Lemma 4.8 are valid in $\mathfrak{A}$. This gives an alternative (non-equational) axiomatization of the theory of relation algebras.

4.27. Show that $\mathfrak{A} = (A\,,+\,,-\,,;\,,{}^{\smile}\,,1')$ is a relation algebra if and only if (R1)–(R6) and the following three laws are valid in $\mathfrak{A}$.

(i) $r\,;0 = 0$.
(ii) $0\,;r = 0$.
(iii) $(r\,;s)\cdot t \le [r\cdot(t\,;s^{\smile})]\,;[s\cdot(r^{\smile}\,;t)]$.

This gives an alternative equational axiomatization of the theory of relation algebras.

4.28. Show that the following are equivalent in any algebra

$$\mathfrak{A} = (A\,,+\,,-\,,;\,,{}^{\smile}\,,1')$$

that satisfies (R1)–(R9).

(i) Axiom (R10) is valid in $\mathfrak{A}$.
(ii) The laws $r^{\smile} ; -r \leq 0'$ and $r^{\smile} ; -(r ; 1) = 0$ are valid in $\mathfrak{A}$.
(iii) For every element r in $\mathfrak{A}$, the largest element s satisfying the inequality $s ; -r \leq 0'$ is $r^{\smile}$.

This result yields two other possible axiomatizations of the theory of relation algebras.

4.29. Prove that the following equivalences hold in all relation algebras.

(i) $r ; s \leq 0'$ if and only if $r^{\smile} \cdot s = 0$.
(ii) $r ; s^{\smile} \leq 0'$ if and only if $r \cdot s = 0$.

4.30. Use Exercise 4.29 to give an alternative proof of Lemma 4.14.

4.31. An element r is called an *equivalence element* if

$$r^{\smile} \leq r \qquad \text{and} \qquad r ; r \leq r.$$

Prove that the equation in Lemma 4.34 holds with an arbitrary equivalence element in place of 0'.

4.32. Prove that a relation algebra is degenerate if and only if the equation $0 = 1'$ is true in it.

Chapter 5
Special elements

We now turn to the study of more specialized laws. As was seen in Section 1.4, special properties of binary relations such as symmetry or functionality can often be expressed by means of equations in the language of relation algebras, and it is natural to formulate and study laws that apply to elements satisfying abstract versions of these properties. In the first three sections below, we look at abstract versions of properties associated with symmetric relations, transitive relations, and equivalence relations. In subsequent sections, we look at abstract versions of properties associated with various types of ideal elements, with rectangles, and with functions. As in Chapter 4, we assume that all elements under discussion belong to a fixed relation algebra $\mathfrak{A}$, which we shall usually not bother to mention explicitly.

5.1 Symmetric elements

Symmetric elements are relation algebraic abstractions of symmetric relations, discussed in Section 1.4. An element r is said to be *symmetric* if $r^{\smile} \leq r$. These elements can be characterized in several different ways.

Lemma 5.1. *The following conditions on an element* r *are equivalent.*

(i) r *is symmetric.*
(ii) $r^{\smile} = r$.
(iii) $r = s + s^{\smile}$ *for some element* s.

Proof. If (i) holds, then $r^{\smile} \leq r$, by definition, and therefore

S. Givant, *Introduction to Relation Algebras*,
DOI 10.1007/978-3-319-65235-1_5

$$r = r^{\smile\smile} \leq r^{\smile},$$

by the first involution law and the monotony law for converse. It follows from these inequalities that (ii) holds. The reverse implication from (ii) to (i) is trivial.

If (ii) holds, then $r = r + r = r + r^{\smile}$, so (iii) holds. On the other hand, if (iii) holds, then

$$r^{\smile} = (s + s^{\smile})^{\smile} = s^{\smile} + s^{\smile\smile} = s^{\smile} + s = r,$$

by the distributive law for converse, the first involution law, and Boolean algebra, so (ii) holds. □

The equivalence of (i) and (ii) in the preceding lemma implies that the symmetric elements in a relation algebra $\mathfrak{A}$ are just the fixed points of the Boolean automorphism of $\mathfrak{A}$ that maps each element to its converse. The equivalence of (i) and (iii) implies that there is a polynomial whose range is precisely the set of symmetric elements in $\mathfrak{A}$, namely the function ψ defined on $\mathfrak{A}$ by

$$\psi(s) = s + s^{\smile}.$$

The following lemma contains some of the basic closure properties of the set of symmetric elements.

Lemma 5.2. (i) *The distinguished constants* 0, 1, 1', *and* 0' *are symmetric.*
(ii) *If r is symmetric, then so is $-r$.*
(iii) *The sum of a set of symmetric elements, if it exists, is symmetric. In particular, if r and s are symmetric, then so is $r + s$.*
(iv) *The product of a set of symmetric elements, if it exists, is symmetric. In particular, if r and s are symmetric, then so is $r \cdot s$.*
(v) *If r is symmetric, then so is $r^{\smile}$.*
(vi) *If r and s are symmetric, then the relative product $r ; s$ is symmetric if and only if $r ; s = s ; r$.*
(vii) *If r and s are symmetric, then the relative sum $r \mathbin{+\!\!,} s$ is symmetric if and only if $r \mathbin{+\!\!,} s = s \mathbin{+\!\!,} r$.*

Proof. The elements 1' and 0' are symmetric by Lemma 4.3 and its second dual, Lemma 4.7(vi). The remainder of part (i), and all of parts (ii)–(iv), follow from the observation made above that symmetric elements are fixed points of the Boolean automorphism φ mapping

each element to its converse. For example, if X is a set of symmetric elements such that the product $t = \prod X$ exists, then $\varphi(r) = r$ for each r in X, and therefore

$$\varphi(t) = \varphi(\prod X) = \prod\{\varphi(r) : r \in X\} = \prod\{r : r \in X\} = t,$$

by the Boolean automorphism properties of φ. This computation shows that t is a fixed point of φ and therefore a symmetric element, which proves (iv).

Part (v) is trivial, and parts (vi) and (vii) are consequences of the second involution law and its second dual, Lemma 4.7(iii). For example, if r and s are symmetric elements, then

$$(r \mathbin{;} s)^{\smile} = s^{\smile} \mathbin{;} r^{\smile} = s \mathbin{;} r,$$

by the second involution law and Lemma 5.1(ii). Consequently,

$$r \mathbin{;} s = (r \mathbin{;} s)^{\smile} \qquad \text{if and only if} \qquad r \mathbin{;} s = s \mathbin{;} r,$$

which proves (vi). □

A relation algebra is said to be *abelian*, or *commutative*, if

$$r \mathbin{;} s = s \mathbin{;} r$$

for all elements r and s in the algebra. In an abelian relation algebra, the set of symmetric elements contains the distinguished constants, by part (i) of Lemma 5.2, and it is closed under the operations of the algebra, by parts (ii)–(vi) of that lemma. A subset of a relation algebra with these properties is called a *subuniverse* (see Chapter 6). Thus, the set of symmetric elements is always a subuniverse of an abelian relation algebra.

A relation algebra is said to be *symmetric* if $r^{\smile} = r$ for each element r in the algebra. Every complex algebra of a geometry is an example of a relation algebra that is abelian and symmetric, as is every complex algebra of a Boolean group, that is to say, a group in which every element is its own inverse. The complex algebra of an abelian group that is not a Boolean group is an example a relation algebra that is abelian but not symmetric. The following consequence of Lemma 5.2(vi) asserts that symmetry implies commutativity.

Corollary 5.3. *Every symmetric relation algebra is abelian.*

5.2 Transitive elements

Transitive elements and reflexive elements are relation algebraic abstractions of transitive relations and reflexive relations, discussed in Section 1.4. An element r is said to be *transitive* if $r \mathbin{;} r \leq r$, and *reflexive* if $1' \leq r$. There are a number of interesting characterizations of transitive elements. Before stating these characterizations, we make a preliminary observation.

Lemma 5.4. *The elements $s \mathbin{\underset{,}{+}} (-s)^{\smile}$ and $(-s)^{\smile} \mathbin{\underset{,}{+}} s$ are transitive for any element s.*

Proof. Write $r = s \mathbin{\underset{,}{+}} (-s)^{\smile}$, and observe that

$$\begin{aligned} r \mathbin{;} r &= [s \mathbin{\underset{,}{+}} (-s)^{\smile}] \mathbin{;} [s \mathbin{\underset{,}{+}} (-s)^{\smile}] \leq s \mathbin{\underset{,}{+}} [(-s)^{\smile} \mathbin{;} (s \mathbin{\underset{,}{+}} (-s)^{\smile})] \\ &\leq s \mathbin{\underset{,}{+}} [(-s)^{\smile} \mathbin{;} s] \mathbin{\underset{,}{+}} (-s)^{\smile} \leq s \mathbin{\underset{,}{+}} 0' \mathbin{\underset{,}{+}} (-s)^{\smile} = s \mathbin{\underset{,}{+}} (-s)^{\smile} = r, \end{aligned}$$

by the definition of r, Lemma 4.28 (with s, $(-s)^{\smile}$, and $s \mathbin{\underset{,}{+}} (-s)^{\smile}$ in place of r, s, and t respectively), Corollary 4.29 (with $(-s)^{\smile}$ in place of r and t), Lemma 4.12 (with $-s$ in place of r), and the monotony and identity laws for relative addition. This argument shows that r is transitive. A dual argument shows that $(-s)^{\smile} \mathbin{\underset{,}{+}} s$ is transitive. □

We turn now to some characterizations of transitive elements. One of them requires a bit of notation. For an arbitrary element r, define the *power* r^n by induction on natural numbers n as follows:

$$r^0 = 1' \qquad \text{and} \qquad r^{n+1} = r^n \mathbin{;} r.$$

Observe that $r^1 = r^0 \mathbin{;} r = 1' \mathbin{;} r = r$. It is easy to check that various well-known laws concerning exponentiation continue to hold in this setting. For example,

$$r^m \mathbin{;} r^n = r^{m+n} \qquad \text{and} \qquad (r^m)^n = r^{mn}.$$

Such expressions as $\sum_{n=i}^{j} r^n$ will have their usual meaning,

$$\textstyle\sum_{n=i}^{j} r^n = r^i + r^{i+1} + \cdots + r^j,$$

except that addition is to be interpreted as Boolean addition. The expression $\sum_{n=1}^{\infty} r^n$ is to be interpreted as the supremum of the set $\{r^n : n \geq 1\}$.

Lemma 5.5. *The following conditions on an element* r *are equivalent.*

(i) r *is transitive.*
(ii) $r \leq (-r)^{\smile} +\!\!\!\!, \, r$.
(iii) $r \leq r +\!\!\!\!, \,(-r)^{\smile}$.
(iv) $r^{\smile} ; -r \leq -r$.
(v) $-r ; r^{\smile} \leq -r$.
(vi) $r = s \cdot [(-s)^{\smile} +\!\!\!\!, \, s]$ *for some element* s.
(vii) $r = s \cdot [s +\!\!\!\!, \,(-s)^{\smile}]$ *for some element* s.
(viii) $r = \sum_{n=1}^{\infty} s^n$ *for some element* s.

Proof. The proof proceeds by establishing the equivalence of the pairs of conditions (i) and (iv), (iv) and (ii), (i) and (v), (v) and (iii), and (i) and (viii); and the implications from (ii) to (vi), from (vi) to (i), from (iii) to (vii), and from (vii) to (i). The equivalence of (i) and (iv) is a consequence of Boolean algebra and the De Morgan-Tarski laws:

$$\begin{aligned} r ; r \leq r \qquad & \text{if and only if} \qquad (r ; r) \cdot -r = 0, \\ & \text{if and only if} \qquad (r^{\smile} ; -r) \cdot r = 0, \\ & \text{if and only if} \qquad r^{\smile} ; -r \leq -r. \end{aligned}$$

An analogous argument establishes the equivalence of (i) and (v). To establish the equivalence of (ii) and (iv), form the complement of each side of the inequality in (iv), and apply Boolean algebra, the definition of relative addition, and Lemma 4.1(v) to obtain (ii); and proceed in an analogous fashion to obtain (iv) from (ii) . A similar argument shows that (iii) and (v) are equivalent.

If (ii) holds, take s to be r to see that (vi) must hold. Assume now that (vi) holds, with the goal of showing that (i) must hold. First of all,

$$\begin{aligned} r ; r &= (s \cdot [(-s)^{\smile} +\!\!\!\!, \, s]) ; (s \cdot [(-s)^{\smile} +\!\!\!\!, \, s]) \\ &\leq [(-s)^{\smile} +\!\!\!\!, \, s] ; [(-s)^{\smile} +\!\!\!\!, \, s] \leq (-s)^{\smile} +\!\!\!\!, \, s, \end{aligned} \tag{1}$$

by the assumption in (vi), the monotony law for relative multiplication, and Lemma 5.4. Also,

$$r ; r = (s \cdot [(-s)^{\smile} +\!\!\!\!, \, s]) ; (s \cdot [(-s)^{\smile} +\!\!\!\!, \, s]) \leq s ; [(-s)^{\smile} +\!\!\!\!, \, s] \leq s, \tag{2}$$

by the assumption in (vi), the monotony law for relative multiplication, and the first dual of the first inequality in Corollary 4.30 (with s and $-s$

in place of r and s respectively). Combine (1) and (2) to arrive at the desired conclusion:

$$r ; r \leq s \cdot [(-s)^{\smile} \mathbin{+\!\!\!,} s] = r.$$

An analogous argument shows that (iii) implies (vii), which in turn implies (i). Thus, (i)–(vii) are all equivalent.

To complete the proof, it remains to establish the equivalence of (i) and (viii). If r is transitive, then an easy inductive argument shows that $r^n \leq r$ for every positive integer n, so that

$$r = \sum_{n=1}^{\infty} r^n.$$

Take s in (viii) to be r to see that (viii) holds. On the other hand, if (viii) holds, then

$$r ; r = \Big(\sum_{n=1}^{\infty} s^n\Big) ; \Big(\sum_{n=1}^{\infty} s^n\Big) = \sum_{m,n\geq 1} (s^m ; s^n) = \sum_{n=2}^{\infty} s^n \leq r,$$

by the definition of r, the complete distributivity of relative multiplication, and the exponential laws mentioned before the lemma. Consequently, (i) holds. □

The equivalence of (i) and (vi) in the preceding lemma implies that there is a polynomial whose range is precisely the set of transitive elements in a relation algebra $\mathfrak{A}$, namely the function ψ defined on $\mathfrak{A}$ by

$$\psi(s) = s \cdot [(-s)^{\smile} \mathbin{+\!\!\!,} s].$$

In view of Lemma 5.1, it is natural to ask whether the simpler function ϑ defined by

$$\vartheta(s) = (-s)^{\smile} \mathbin{+\!\!\!,} s$$

has the same property. It is not too difficult to check that this is in fact not the case. The details are left as an exercise.

To clarify the significance of part (viii) of the preceding lemma, consider an arbitrary element s (in a fixed relation algebra), and let t be a transitive element such that $s \leq t$. An easy argument by induction, using the monotony law for relative multiplication, shows that $s^n \leq t$ for every positive integer $n \geq 1$. Consequently, if r is the sum of

the powers s^n for $n \geq 1$—as in part (viii) of the preceding lemma—then $r \leq t$. Conclusion: for every element s in a countably complete relation algebra (a relation algebra in which the supremum of every countable subset exists), there is a smallest transitive element r with the property that $s \leq r$. This element r is called the *transitive closure* of s, and it is determined by the equation in (viii). (The assumption of countable completeness is needed to ensure the existence of the sum in (viii) for every element s.) There is also a smallest reflexive and transitive element r^* such that $s \leq r^*$, namely the element r^* determined by the formula

$$r^* = \sum_{n=0}^{\infty} s^n.$$

The following lemma states some of the basic closure properties of the set of transitive elements.

Lemma 5.6. (i) *The distinguished constants* 0, 1*, and* 1' *are transitive.*

(ii) *The product of a set of transitive elements, if it exists, is transitive. In particular, if r and s are transtive, then so is $r \cdot s$.*

(iii) *If r is transitive, then so is $r^{\smile}$.*

(iv) *If r and s are transitive, and if $r ; s = s ; r$, then $r ; s$ is transitive.*

Proof. Part (i) follows from Corollary 4.17, Lemma 4.5(iv), and the identity law for relative multiplication, while part (iii) is a consequence of the monotony law for converse and the second involution law. For part (ii), consider a set X of transitive elements such that the product $t = \prod X$ exists. If r is any element in X, then r is transitive, by assumption, and $t \leq r$, by the definition of t, so

$$t ; t \leq r ; r \leq r.$$

Consequently, $t ; t$ is a lower bound of the set X. The element t is, by assumption, the greatest lower bound of X, so $t ; t \leq t$.

For part (iv), observe that if $r ; s = s ; r$, then

$$(r ; s) ; (r ; s) = (r ; r) ; (s ; s) \leq r ; s,$$

by the associative and monotony laws for relative multiplication, and the assumption that r and s are transitive. It follows that $r ; s$ is transitive. □

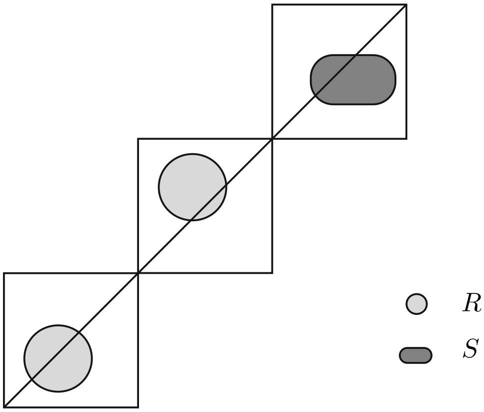


Fig. 5.1 Strongly disjoint relations R and S.

The sum of a set of transitive elements is in general not transitive, but there are some exceptions when the elements in the set have certain special properties with respect to one another. A set X of elements is said to be *directed* if for every r and s in X, there is a t in X such that $r \leq t$ and $s \leq t$; and X is said to be *strongly disjoint* if

$$(r ; 1) \cdot (1 ; s) = 0$$

for every pair of distinct elements r and s in X. In a set relation algebra with unit E, two relations R and S are strongly disjoint just in case the elements in the field of R (the union of the domain and range of R) come from entirely different equivalence classes of E than the elements in the field of S (see Figure 5.1).

Lemma 5.7. (i) *The sum of a directed set of transitive elements, if it exists, is transitive.*

(ii) *The sum of a strongly disjoint set of transitive elements, if it exists, is transitive. In particular, if r and s are transitive and strongly disjoint, then $r + s$ is transitive.*

Proof. Consider a set X of transitive elements for which the sum

$$t = \sum X$$

exists. Apply the complete distributivity law for relative multiplication (Corollary 4.18) to obtain

$$t ; t = (\sum X) ; (\sum X) = \sum\{r ; s : r, s \in X\}. \tag{1}$$

If the set X is directed, then for every r and s in X, there is a p in X such that $r \leq p$ and $s \leq p$, and therefore

$$r ; s \leq p ; p \leq p, \tag{2}$$

by the monotony law for relative multiplication and the assumption that p is transitive. Combine (1) and (2) to arrive at

$$t ; t = \sum\{r ; s : r, s \in X\} \leq \sum\{p : p \in X\} = t.$$

If the set X is strongly disjoint, then since

$$r ; s \leq r ; 1 \qquad \text{and} \qquad r ; s \leq 1 ; s,$$

by the monotony law for relative multiplication, we have

$$r ; s \leq (r ; 1) \cdot (1 ; s) = 0 \tag{3}$$

for all distinct elements r and s in X. Consequently,

$$t ; t = \sum\{r ; s : r, s \in X\} = \sum\{r ; r : r \in X\} \leq \sum\{r : r \in X\} = t,$$

by (1), (3), the assumed transitivity of the elements in X, and the definition of t. Thus, in either of the two cases under consideration, the element t is transitive. □

5.3 Equivalence elements

An element r that is symmetric and transitive is called an *equivalence element*. Notice that r is not required to be *reflexive* in the sense that $1' \leq r$. In the full set relation algebra on a set U, the equivalence elements are the equivalence relations on subsets of U (see Figure 5.2) rather than the equivalence relations on the set U itself. The reason for the somewhat greater generality in the definition is that equivalence elements of this more general type play an important role in the study of algebraic properties of relation algebras. Equivalence elements r with the property that $1' \leq r$ are called *reflexive equivalence elements*.

There are several useful characterizations of equivalence elements.

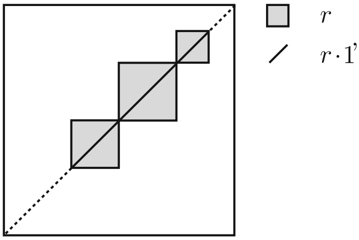


Fig. 5.2 A typical set-theoretic equivalence element r, and the portion of 1' that is included in r.

Lemma 5.8. *The following conditions on an element r are equivalent.*

(i) r *is an equivalence element.*
(ii) $r^{\smile} = r$ *and* $r \mathbin{;} r = r$.
(iii) $r \mathbin{;} r^{\smile} = r$.
(iv) $r^{\smile} \mathbin{;} r = r$.
(v) $r \mathbin{;} r^{\smile} \leq r$ *and* $r^{\smile} \mathbin{;} r \leq r$.
(vi) $r \mathbin{;} -r \leq -r$ *and* $-r \mathbin{;} r \leq -r$.
(vii) $r = s \cdot s^{\smile} \cdot [(-s)^{\smile} \mathbin{\underset{,}{+}} s] \cdot [s^{\smile} \mathbin{\underset{,}{+}} -s]$ *for some element* s.
(viii) $r = s \cdot s^{\smile} \cdot [s \mathbin{\underset{,}{+}} (-s)^{\smile}] \cdot [-s \mathbin{\underset{,}{+}} s^{\smile}]$ *for some element* s.
(ix) $r = \sum_{n=1}^{\infty}(s + s^{\smile})^n$ *for some element* s.

Proof. We establish the equivalence of (i) and (ii); the implications from (ii) to (iii), (iv), and (v); the implications from (iii) to (ii) and (iv); the implications from (iv) to (ii) and (iii); the implication from (v) to (iv); the equivalence of (v) and (vi); the equivalence of (i) and (vii); the equivalence of (i) and (viii); and the equivalence of (i) and (ix).

If r is symmetric and transitive, then $r^{\smile} = r$, by Lemma 5.1, and

$$r \leq r \mathbin{;} r^{\smile} \mathbin{;} r \leq r \mathbin{;} r \mathbin{;} r \leq r \mathbin{;} r \leq r,$$

by Corollary 4.22, the symmetry and transitivity of r, and the monotony law for relative multiplication. Since the first and last terms are equal, equality must hold everywhere, and in particular $r \mathbin{;} r = r$. Consequently, (i) implies (ii), while the reverse implication is trivial.

It is clear that (ii) implies each of (iii), (iv), and (v). Suppose now that (iii) holds. Form the converse of both sides of (iii), and apply the second and first involution laws, to arrive at

$$r^{\smile} = (r \mathbin{;} r^{\smile})^{\smile} = r^{\smile\smile} \mathbin{;} r^{\smile} = r \mathbin{;} r^{\smile} = r.$$

Thus, r is equal to its own converse, so (iii) obviously implies (ii) and (iv). A completely analogous argument shows that (iv) implies (ii) and (iii).

Suppose next that condition (v) holds. Take the converse of both sides of the first inequality in (v), and use the monotony law for relative multiplication and the two involution laws, to obtain

$$r^{\smile} \geq (r \mathbin{;} r^{\smile})^{\smile} = r^{\smile\smile} \mathbin{;} r^{\smile} = r \mathbin{;} r^{\smile}. \tag{1}$$

Consequently,

$$r \leq r \mathbin{;} r^{\smile} \mathbin{;} r \leq r^{\smile} \mathbin{;} r \leq r, \tag{2}$$

by Corollary 4.22, (1), and the second inequality in (v). Since the first and last terms in (2) are the same, equality must hold everywhere, and in particular $r = r^{\smile} \mathbin{;} r$. Thus, (v) implies (iv).

The equations

$$(r \mathbin{;} -r) \cdot r = 0 \qquad \text{and} \qquad (r^{\smile} \mathbin{;} r) \cdot -r = 0$$

are equivalent, by the De Morgan-Tarski laws (with s and t replaced by $-r$ and r respectively). The first equation is equivalent to the first inequality in (vi), while the second equation is equivalent to the second inequality in (v), by Boolean algebra. Thus, the second inequality in (v) is equivalent to the first inequality in (vi). A similar remark applies to the first inequality in (v) and the second inequality in (vi), so (v) and (vi) are equivalent.

Turn now to the equivalence of (i) and (vii). Observe first of all that for any element s,

$$(s \cdot [(-s)^{\smile} \mathbin{\underset{,}{+}} s])^{\smile} = s^{\smile} \cdot [(-s)^{\smile} \mathbin{\underset{,}{+}} s]^{\smile} = s^{\smile} \cdot (s^{\smile} \mathbin{\underset{,}{+}} -s), \tag{3}$$

by Lemma 4.1(ii) and the involution laws. If r is an equivalence element, then r is transitive and symmetric, so

$$r = r \cdot [(-r)^{\smile} \mathbin{\underset{,}{+}} r], \tag{4}$$

by Lemma 5.5(ii), and therefore

$$r = r^{\smile} = (r \cdot [(-r)^{\smile} \mathbin{\underset{,}{+}} r])^{\smile} = r^{\smile} \cdot (r^{\smile} \mathbin{\underset{,}{+}} -r),$$

by (4) and (3) (with r in place of s). It follows that (vii) holds if s is taken to be r, so (i) implies (vii).

To establish the reverse implication, assume that (vii) holds for some element s. Write $p = s \cdot [(-s)^{\smile} \mathbin{+\!\!,} s]$, and observe that

$$p^{\smile} = s^{\smile} \cdot (s^{\smile} \mathbin{+\!\!,} -s) \qquad \text{and} \qquad r = p \cdot p^{\smile}, \tag{5}$$

by (3) and (vii). The element p is transitive, by Lemma 5.5(vi), so its converse $p^{\smile}$ is transitive, by Lemma 5.6(iii). The product $p \cdot p^{\smile}$ is therefore transitive, by Lemma 5.6(ii), and this product is symmetric, by Lemma 4.1(ii) and the first involution law. Thus, r is an equivalence element, by the second equation in (5).

The proof that (i) and (viii) are equivalent is similar, but uses (iii) and (vii) from Lemma 5.5 instead of (ii) and (vi).

The proof that (i) and (ix) are equivalent is more straightforward. If r is an equivalence element, then $r = r^{\smile} = r \mathbin{;} r$, by part (ii) of the lemma, so an easy argument by induction shows that $r = (r + r^{\smile})^n$ for every positive integer n. Consequently, the equation in (ix) holds with r in place of s. To establish the reverse implication, assume that r can be written in the form (ix) for some element s. The element $s + s^{\smile}$ is symmetric, by Lemma 5.1(iii), so an easy argument by induction—using also Lemma 5.2(vi)—shows that $(s + s^{\smile})^n$ is symmetric for every positive integer n. Therefore, the element r must be symmetric, by Lemma 5.2(iii). Notice that r is transitive, by Lemma 5.5(viii), so r is an equivalence element. □

The equivalence of (i) and (vii) in the preceding lemma implies that there is a polynomial whose range is precisely the set of equivalence elements in a relation algebra $\mathfrak{A}$, namely the function ψ defined on $\mathfrak{A}$ by

$$\psi(s) = s \cdot s^{\smile} \cdot [(-s)^{\smile} \mathbin{+\!\!,} s] \cdot [s^{\smile} \mathbin{+\!\!,} -s].$$

The equivalence of (i) and (ix) implies that for every element s in a countably complete relation algebra, there is a smallest equivalence element r with the property that $s \le r$. This element r may be called the *equivalence closure*, or the *symmetric-transitive closure*, of s, and it is determined by the equation in (ix). There is also a smallest reflexive equivalence element r^* such that $s \le r^*$, namely the element determined by the formula

$$r^* = \sum_{n=0}^{\infty} (s + s^{\smile})^n.$$

Lemmas 5.2, 5.6, and 5.7 apply in particular to equivalence elements and imply the following closure properties of the set of equivalence elements.

Lemma 5.9. (i) *The distinguished constants* 0, 1, *and* 1' *are equivalence elements.*
(ii) *The product of a set of equivalence elements, if it exists, is an equivalence element. In particular, if* r *and* s *are equivalence elements, then so is* $r \cdot s$.
(iii) *The sum of a directed set of equivalence elements, if it exists, is an equivalence element.*
(iv) *The sum of a strongly disjoint set of equivalence elements, if it exists, is an equivalence element.*
(v) *If* r *and* s *are equivalence elements, then* $r\,;s$ *is an equivalence element if and only if* $r\,;s = s\,;r$.

The product of two equivalence elements is always below their relative product.

Corollary 5.10. *If* r *and* s *are equivalence elements, then* $r \cdot s \le r\,;s$.

Proof. If r and s are equivalence elements, then $r \cdot s$ is an equivalence element, by Lemma 5.9(ii), and therefore

$$r \cdot s = (r \cdot s)\,;(r \cdot s) \le (r\,;r)\,;(s\,;s) = r\,;s,$$

by Lemmas 5.8(ii) and 4.5(ii). □

Not only is the identity element 1' an equivalence element, but also every element that is below 1'. Such elements are called *subidentity elements*, and of course elements below 0' are called *subdiversity elements*.

Lemma 5.11. *If* $r \le 1'$, *then* r *is an equivalence element.*

Proof. If $r \le 1'$, then

$$r\,;-r \le 1'\,;-r = -r \qquad \text{and} \qquad -r\,;r \le -r\,;1' = -r,$$

by the monotony and identity laws for relative multiplication. Apply Lemma 5.8(vi) to conclude that r is an equivalence element. □

Although the diversity element is in general not an equivalence element, the square of the diversity element, that is to say, the element $0'\,;0'$, is an equivalence element, by Lemmas 4.34 and 4.7(vi) (together with the second involution law). This interesting result can be generalized.

Lemma 5.12. *If r is an equivalence element, then so is $-r \mathbin{;} -r$.*

Proof. Assume r is an equivalence element. The product $-r \mathbin{;} -r$ is symmetric, by Lemma 5.2(ii),(vi), so it remains to prove that $-r \mathbin{;} -r$ is transitive. Observe that

$$-r \mathbin{+\!\!\!,} -r = -(r \mathbin{;} r) = -r, \tag{1}$$

by the definition of relative addition, Boolean algebra, Lemma 5.8(ii), and the assumption that r is transitive. Consequently,

$$-r \mathbin{;} -r = -r \mathbin{;} (-r \mathbin{+\!\!\!,} -r) \leq -r \mathbin{;} -r \mathbin{+\!\!\!,} -r, \tag{2}$$

by (1) and the semi-modular law in Corollary 4.29. Form the relative product of the first and last terms in (2) with $-r$ on the right, and use the monotony law for relative multiplication and the semi-modular law in Lemma 4.28 to obtain

$$-r \mathbin{;} -r \mathbin{;} -r \leq (-r \mathbin{;} -r \mathbin{+\!\!\!,} -r) \mathbin{;} -r \leq -r \mathbin{;} -r \mathbin{+\!\!\!,} -r \mathbin{;} -r. \tag{3}$$

Form the relative product of the first and last terms in (3) with $-r$ on the right, and use the monotony law for relative multiplication, the semi-modular law in Lemma 4.28, (3), and the monotony law for relative addition to arrive at

$$\begin{aligned} -r \mathbin{;} -r \mathbin{;} -r \mathbin{;} -r &\leq (-r \mathbin{;} -r \mathbin{+\!\!\!,} -r \mathbin{;} -r) \mathbin{;} -r \\ &\leq -r \mathbin{;} -r \mathbin{+\!\!\!,} -r \mathbin{;} -r \mathbin{;} -r \\ &\leq -r \mathbin{;} -r \mathbin{+\!\!\!,} -r \mathbin{;} -r \mathbin{+\!\!\!,} -r \mathbin{;} -r. \end{aligned} \tag{4}$$

The element $-r \mathbin{;} -r$ is symmetric, so it is equal to its own converse, by Lemma 5.1(ii). Use this observation and the second dual of Corollary 4.22 (with $-r \mathbin{;} -r$ in place of r), to obtain

$$\begin{aligned} &(-r \mathbin{;} -r) \mathbin{+\!\!\!,} (-r \mathbin{;} -r) \mathbin{+\!\!\!,} (-r \mathbin{;} -r) \\ &\qquad = (-r \mathbin{;} -r) \mathbin{+\!\!\!,} (-r \mathbin{;} -r)^{\smile} \mathbin{+\!\!\!,} (-r \mathbin{;} -r) \leq -r \mathbin{;} -r. \end{aligned} \tag{5}$$

Combine (4) and (5) to conclude that

$$(-r \mathbin{;} -r) \mathbin{;} (-r \mathbin{;} -r) \leq -r \mathbin{;} -r$$

and therefore $-r \mathbin{;} -r$ is transitive. □

There are two very useful modular laws that are applicable to equivalence elements. The next lemma gives one form of the first of these laws.

Lemma 5.13. *If r is an equivalence element, then $t \le r$ implies*

$$r \cdot (s \,;\, t) = (r \cdot s) \,;\, t.$$

Proof. Assume $t \le r$. Use the monotony laws for relative multiplication and converse, the assumption that r is an equivalence element, and Lemma 5.8 to obtain

$$r \,;\, t \le r \,;\, r = r \qquad \text{and} \qquad r \,;\, t^{\smile} \le r \,;\, r^{\smile} = r.$$

These inequalities show that the hypotheses of the modular law in Corollary 4.33 are satisfied. Apply that corollary to arrive at the desired conclusion. □

The preceding modular law and its first dual can also be written in the form of equations, and in fact these equations characterize equivalence elements.

Lemma 5.14. *An element r is an equivalence element if and only if*

$$r \cdot [s \,;\, (r \cdot t)] = (r \cdot s) \,;\, (r \cdot t) \quad \textit{and} \quad [(t \cdot r) \,;\, s] \cdot r = (t \cdot r) \,;\, (s \cdot r)$$

for all elements s and t.

Proof. If r is an equivalence element, then the given equations hold, by Lemma 5.13 and its first dual (with $r \cdot t$ in place of t). To establish the reverse implication, use Boolean algebra, the first of the given modular laws (with $-r$ and r in place of s and t respectively), and the first dual of Corollary 4.17 to obtain

$$r \cdot (-r \,;\, r) = r \cdot [-r \,;\, (r \cdot r)] = (r \cdot -r) \,;\, (r \cdot r) = 0 \,;\, r = 0. \tag{1}$$

A dual argument using the second of the given modular laws yields

$$(r \,;\, -r) \cdot r = 0. \tag{2}$$

The equations in (1) and (2) imply the inequalities

$$-r \,;\, r \le -r \qquad \text{and} \qquad r \,;\, -r \le -r,$$

which in turn imply that r is an equivalence element, by Lemma 5.8(vi). □

The second modular law to be discussed is very similar in the form to the first modular law, as formulated in Lemma 5.14, but the roles of Boolean and relative multiplication are reversed. The proof uses the first dual of Corollary 4.33, which may be written in the form

$$t\,;r \le r \quad \text{and} \quad t^{\smile}\,;r \le r \quad \text{implies} \quad (t\,;s)\cdot r = t\,;(s\cdot r).$$

Lemma 5.15. *An element r is an equivalence element if and only if*

$$r\,;[s\cdot(r\,;t)] = (r\,;s)\cdot(r\,;t) \quad \textit{and} \quad [(t\,;r)\cdot s]\,;r = (t\,;r)\cdot(s\,;r)$$

for all elements s and t.

Proof. To establish the implication from left to right, assume that r is an equivalence element, and let s and t be arbitrary elements. It suffices, by the first duality principle, to derive the first of the given modular laws. Observe that

$$r\,;(r\,;t) = (r\,;r)\,;t = r\,;t \;\text{ and }\; r^{\smile}\,;(r\,;t) = (r^{\smile}\,;r)\,;t = r\,;t, \quad (1)$$

by the associative law for relative multiplication, Lemma 5.8(ii),(iv), and the assumption that r is an equivalence element. These equations show that the hypotheses of the first dual of Corollary 4.33 (with $r\,;t$ and r in place of r and t respectively) are satisfied. Apply this first dual to arrive at

$$(r\,;s)\cdot(r\,;t) = r\,;[s\cdot(r\,;t)].$$

To establish the reverse implication, use Corollary 4.17, Boolean algebra, the identity law for relative multiplication, and the first of the given modular laws (with $-r$ and 1' in place of s and t respectively) to obtain

$$\begin{aligned} 0 = r\,;0 = r\,;(-r\cdot r) &= r\,;[-r\cdot(r\,;1')] \\ &= (r\,;-r)\cdot(r\,;1') = (r\,;-r)\cdot r. \quad (2) \end{aligned}$$

A dual argument using the second of the given modular laws implies that

$$0 = r\cdot(-r\,;r). \quad (3)$$

As in the proof of Lemma 5.14, the equations in (2) and (3), together with Lemma 5.8(vi), imply that r is an equivalence element. □

We pause in our study of laws involving equivalence elements to give an interesting application of Lemma 5.14. In certain situations, the reflexive equivalence elements in a relation algebra form a modular lattice.

Theorem 5.16. *If a non-empty set L of reflexive equivalence elements in a relation algebra is closed under relative and Boolean multiplication, then L is a modular lattice under the join operation of relative multiplication and the meet operation of multiplication.*

Proof. Consider a non-empty set L of reflexive equivalence elements in a relation algebra $\mathfrak{A}$, and suppose that L is closed under relative and Boolean multiplication. In order to prove that L is a lattice under the join operation $;$ and the meet operation $\cdot$, it suffices to show that for any elements r and s in L, the relative product $r\,;s$ is the least upper bound of r and s in L, and the product $r\cdot s$ is the greatest lower bound of r and s in L. The second of these properties is trivial, since $r \cdot s$ is the greatest lower bound of r and s in $\mathfrak{A}$, by Boolean algebra. To establish the first property, observe that

$$r = r\,;1\text{'} \leq r\,;s \qquad \text{and} \qquad s = 1\text{'}\,;s \leq r\,;s,$$

by the assumption that r and s are reflexive, and the monotony law for relative multiplication. Thus, $r\,;s$ is an upper bound for r and s. If t is any upper bound for r and s in L, then

$$r\,;s \leq t\,;t \leq t,$$

by the monotony law for relative multiplication, and the assumption that t is in L and hence an equivalence element. It follows that $r\,;s$ is the least upper bound of r and s in L.

To prove that L is a modular lattice under these operations, it must be shown that the modular law

$$(r \wedge t) \vee (s \wedge t) = [(r \wedge t) \vee s] \wedge t,$$

that is to say, the law

$$(r \cdot t)\,;(s \cdot t) = [(r \cdot t)\,;s] \cdot t$$

holds in L. But this law is an immediate consequence of the second modular law in Lemma 5.14 (with r and t interchanged). □

Corollary 5.17. *In an abelian relation algebra, the set of all reflexive equivalence elements is a modular lattice with zero and one. The join operation is relative multiplication, the meet operation is multiplication, zero is the identity element, and one is the unit.*

Proof. The set of all reflexive equivalence elements contains 1’ and 1, and is closed under multiplication and relative multiplication, by parts (i), (ii), and (v) of Lemma 5.9. Apply Theorem 5.16 to arrive at the desired conclusion. □

For an illustration of how Theorem 5.16 may be applied, consider the complex algebra of a group G. The non-zero equivalence elements in $\mathfrak{Cm}(G)$ are just the subgroups of G, and each of these subgroups is reflexive because it contains the identity element of the group. The operation of relative multiplication in $\mathfrak{Cm}(G)$ is complex multiplication, and in general the complex product of two subgroups of G need not be a subgroup. The complex product of two normal subgroups, however, is a normal subgroup, and the intersection of two normal subgroups is also a normal subgroup. Conclusion: the set of all normal subgroups of a group G is a modular lattice with zero and one. The join operation is complex multiplication, the meet operation is intersection, the zero is the trivial subgroup, and the unit is the improper subgroup G.

We resume the study of laws involving equivalence elements, and begin with some auxiliary lemmas that are useful in a variety of other contexts as well. The ultimate goal is a strengthened version of Lemma 5.9(iv).

Lemma 5.18. *Let r be an equivalence element.*

(i) $r = (r \cdot 1’) ; r$.
(ii) $r \cdot 1’ = (r ; 1) \cdot 1’$.
(iii) $r \cdot 1’ = (r ; 1 ; r) \cdot 1’$.
(iv) $r ; 1 = (r \cdot 1’) ; 1$.

Proof. Part (i) is a consequence of the modular law in Lemma 5.13 (with 1’ and r in place of s and t respectively), the identity law for relative multiplication, and Boolean algebra:

$$(r \cdot 1’) ; r = r \cdot (1’ ; r) = r \cdot r = r.$$

To prove (ii), observe that

$$(r ; 1) \cdot 1’ \leq r ; (1 \cdot (r^{\smile} ; 1’)) = r ; r^{\smile} = r,$$

by Lemma 4.19 (with 1 and 1' in place of s and t respectively), Boolean algebra and the identity law for relative multiplication, and Lemma 5.8(iii). Consequently,

$$(r\,;1)\cdot 1' \le r\cdot 1',$$

by Boolean algebra. The reverse inequality holds by Lemma 4.5(iii) and Boolean algebra.

For the proof of (iii), use Lemma 4.26, Boolean algebra, and (ii) together with its first dual:

$$(r\,;1\,;r)\cdot 1' = (r\,;1)\cdot(1\,;r)\cdot 1' = (r\,;1)\cdot 1'\cdot(1\,;r)\cdot 1' = r\cdot 1'.$$

To prove (iv), observe first of all that 1 is an equivalence element, by Lemma 5.9(i). Therefore,

$$(r\cdot 1')\,;1 = [(r\,;1)\cdot 1']\,;1 = (r\,;1)\cdot(1'\,;1) = (r\,;1)\cdot 1 = r\,;1,$$

by (ii), the second modular law in Lemma 5.15 (with 1, 1', and r in place of r, s, and t respectively), the identity law for relative multiplication, and Boolean algebra. □

Together, (i) and its first dual in the preceding lemma say that for an equivalence element r, the product $r\cdot 1'$ acts as a two-sided identity element. Parts (ii)–(iv) and their first duals say in different ways that the field of r coincides with the field of $r\cdot 1'$. The next corollary is a consequence of (i) and the first dual of Corollary 4.17.

Corollary 5.19. *If r is an equivalence element, then*

$$r = 0 \qquad \textit{if and only if} \qquad r\cdot 1' = 0.$$

Subidentity elements are equivalence elements, by Lemma 5.11, and on these elements the Peircean operations coincide with their Boolean analogues.

Lemma 5.20. (i) *If $r \le 1'$ and $s \le 1'$, then $r\,;s = r\cdot s$ and $r^{\smile} = r$.*
(ii) *If $r \le 1'$ and $s \le 1'$, then $(r\,;1)\cdot s = r\cdot s$.*
(iii) *If $r \le 1'$, then $(r\,;1)\cdot r = r$.*

Proof. Assume r and s are below 1'. Both elements are equivalence elements, by Lemma 5.11, so $r^{\smile} = r$, by Lemma 5.8(ii), and $r\cdot s \le r\,;s$, by Corollary 5.10. On the other hand,

$$r\,;s \le r\,;1' = r \qquad \text{and} \qquad r\,;s \le 1'\,;s = s,$$

by the monotony and identity laws for relative multiplication, and consequently, $r\,;s \le r \cdot s$, by Boolean algebra. This proves (i).

For the proof of (ii), observe that

$$(r\,;1) \cdot s = (r\,;1) \cdot 1' \cdot s = r \cdot 1' \cdot s = r \cdot s,$$

by Boolean algebra, the assumption that r and s are below 1', and Lemma 5.18(ii). Part (iii) follows at once from (ii) by taking s to be r. □

Part (ii) of the preceding lemma can be extended to the case when s is not a subidentity element in the following way.

Lemma 5.21. *If* $r \le 1'$, *then* $(r\,;1) \cdot s = r\,;s$.

Proof. The monotony and identity laws for relative multiplication, and the assumption that r is a subidentity element imply that

$$r\,;s \le r\,;1 \qquad \text{and} \qquad r\,;s \le 1'\,;s = s,$$

so $r\,;s \le (r\,;1) \cdot s$. For the reverse inequality, observe that

$$(r\,;1) \cdot s \le r\,;[1 \cdot (r^{\smile}\,;s)] = r\,;r^{\smile}\,;s = r\,;s,$$

by Lemma 4.19 (with 1 and s in place of s and t respectively), Boolean algebra, and Lemmas 5.11 and 5.8(iii). □

A useful fact about equivalence elements is that the relative product of two such elements is zero just in case the elements are disjoint.

Lemma 5.22. *If* r *and* s *are equivalence elements*, *then the following conditions are equivalent*.

(i) $r\,;s = 0$.
(ii) $(r\,;1) \cdot (s\,;1) = 0$.
(iii) $r \cdot s = 0$.

Proof. The equivalence of (i) and (ii) is a consequence of the string of equivalences

$$\begin{aligned}
(r\,;1) \cdot (s\,;1) = 0 \qquad &\text{if and only if} \qquad (r^{\smile}\,;1) \cdot (s\,;1) = 0,\\
&\text{if and only if} \qquad (r^{\smile}\,;1\,;1^{\smile}) \cdot s = 0,\\
&\text{if and only if} \qquad (r^{\smile}\,;1) \cdot s = 0,\\
&\text{if and only if} \qquad (r\,;s) \cdot 1 = 0,\\
&\text{if and only if} \qquad r\,;s = 0.
\end{aligned}$$

The first equivalence uses the assumption that r is an equivalence element and Lemma 5.8(ii); the second uses the equivalence of (i) and (iii) in the De Morgan-Tarski laws (with s, 1, and $r^{\smile} ; 1$ in place of r, s, and t respectively); the third uses Lemmas 4.1(vi) and 4.5(iv); the fourth uses the equivalence of (i) and (ii) in the De Morgan-Tarski laws (with 1 and s in place of s and t respectively), and the fifth uses Boolean algebra.

The implication from (ii) to (iii) is an immediate consequence of the inequalities $r \leq r ; 1$ and $s \leq s ; 1$ (see Lemma 4.5(iii)). To establish the reverse implication, assume that (iii) holds. Use Lemma 5.18(iv), Lemma 4.19 (with $r \cdot 1'$, 1, and $(s \cdot 1') ; 1$ in place of r, s, and t respectively), Boolean algebra, Lemma 5.20(i) (with $r \cdot 1'$ and $s \cdot 1'$ in place of r and s), the assumption that r and s are disjoint, and the first dual of Corollary 4.17 to obtain

$$\begin{aligned}
(r ; 1) \cdot (s ; 1) &= [(r \cdot 1') ; 1] \cdot [(s \cdot 1') ; 1] \\
&\leq (r \cdot 1') ; [1 \cdot ((r \cdot 1')^{\smile} ; (s \cdot 1') ; 1)] \\
&= (r \cdot 1') ; (r \cdot 1')^{\smile} ; (s \cdot 1') ; 1 \\
&= [(r \cdot 1') \cdot (r \cdot 1') \cdot (s \cdot 1')] ; 1 \\
&= (r \cdot s \cdot 1') ; 1 = 0 ; 1 = 0.
\end{aligned}$$

Thus, (ii) holds. □

We come finally to a strengthened version of Lemma 5.9(iv) for equivalence elements.

Lemma 5.23. *The sum of a disjoint set of equivalence elements, if it exists, is an equivalence element. In particular, the sum of two disjoint equivalence elements is an equivalence element.*

Proof. The proof is very similar to the proof of Lemma 5.7(ii). Let X be a disjoint set of equivalence elements such that the sum $t = \sum X$ exists. The sum t is symmetric, by Lemma 5.2(iii). The complete distributivity law for relative multiplication (Corollary 4.18) gives

$$t ; t = (\textstyle\sum X) ; (\sum X) = \sum\{r ; s : r, s \in X\}. \tag{1}$$

Since $r ; s = 0$ for distinct elements r and s in X, by Lemma 5.22 and the assumption that the elements in X are disjoint, it follows from (1) and Lemma 5.8(ii) that

$$t ; t = \textstyle\sum\{r ; r : r \in X\} = \sum\{r : r \in X\} = t,$$

so t is transitive. □

There are several other laws about equivalence elements that play an important role in arithmetic and algebraic investigations of relation algebras. We state three of them in the next lemma. The second and third laws are true only for a certain class of relation algebras that are abstract versions of square set relation algebras. We shall study such relation algebras in detail later on. Suffice it for now to give the definition and the principal characterization of these algebras. A relation algebra $\mathfrak{A}$ is called *simple* if it has more than one element, and if every homomorphism on $\mathfrak{A}$ is either one-to-one or has a one-element range. Simple relation algebras are characterized by the fact that $0 \neq 1$ and $1 ; r ; 1 = 1$ for all non-zero elements r in the algebra (see Theorem 9.2).

Lemma 5.24. *Let r be an equivalence element in a relation algebra $\mathfrak{A}$.*

(i) $-r ; r = -r$ *if and only if r is reflexive.*
(ii) $-r ; -r = r$ *or* $-r ; -r = 1$ *whenever $\mathfrak{A}$ is simple and $r < 1$.*
(iii) $-r ; 1 = 1$ *and* $1 ; -r = 1$ *whenever $\mathfrak{A}$ is simple and $r < 1$.*

Proof. For the proof of (i), observe that if r if reflexive, then

$$-r ; r \leq -r = -r ; 1\text{'} \leq -r ; r, \tag{1}$$

by Lemma 5.8(vi), and the monotony and identity laws for relative multiplication. The first and last terms in (1) are the same, so equality must hold everywhere. In particular, $-r ; r = -r$. On the other hand, if this last equation holds, then

$$-r = -r ; r = -r ; r^{\smile} \leq 0\text{'},$$

by the symmetry of r and the first dual of Lemma 4.12, so $1\text{'} \leq r$ by Boolean algebra.

Assume now that $\mathfrak{A}$ is simple and $r < 1$. The complement $-r$ is not zero, by Boolean algebra, so the assumed simplicity of $\mathfrak{A}$ implies that $1 ; -r ; 1 = 1$. Replace the first occurrence of 1 in this equation by $r + -r$, and use the distributive law for relative multiplication, Lemma 5.8(vi), and the monotony law for relative multiplication to arrive at

$$\begin{aligned} 1 = (r + -r) ; -r ; 1 = r ; -r ; 1 + -r ; -r ; 1 \\ \leq -r ; 1 + -r ; 1 = -r ; 1. \end{aligned} \tag{2}$$

This proves the first equation in (iii). The second equation is the first dual of the first equation.

Turn now to the proof of (ii). Replace the right-most occurrence of 1 in (2) with $r + -r$, and use the distributive law for relative multiplication and Lemma 5.8(vi) to obtain

$$1 = -r\,;(r + -r) = -r\,;r + -r\,;-r \leq -r + -r\,;-r. \tag{3}$$

It follows from (3) and Boolean algebra that $r \leq -r;-r$. There are now two possibilities. If equality holds, then we obtain the first equation in (ii). If equality does not hold, then $(-r\,;-r)\cdot -r$ is different from 0, and therefore

$$1\,;[(-r\,;-r)\cdot -r]\,;1 = 1,$$

by the assumed simplicity of $\mathfrak{A}$. Replace the two occurrences of 1 on the left side of this equation with $r + -r$, and use the distributive law for relative multiplication, to write 1 as the sum of the four terms

$$\begin{array}{rr} r\,;[(-r\,;-r)\cdot -r]\,;r, & r\,;[(-r\,;-r)\cdot -r]\,;-r, \\ -r\,;[(-r\,;-r)\cdot -r]\,;r, & -r\,;[(-r\,;-r)\cdot -r]\,;-r. \end{array}$$

Each of these terms is below $-r\,;-r$, so $-r\,;-r$ must also be equal to 1. For example,

$$r\,;[(-r\,;-r)\cdot -r]\,;r \leq r\,;-r\,;-r\,;r \leq -r\,;-r,$$

by the monotony law for relative multiplication and Lemma 5.8(vi),

$$r\,;[(-r\,;-r)\cdot -r]\,;-r \leq r\,;-r\,;-r \leq -r\,;-r,$$

by the monotony law for relative multiplication and Lemma 5.8(vi), and

$$-r\,;[(-r\,;-r)\cdot -r]\,;-r \leq -r\,;-r\,;-r\,;-r \leq -r\,;-r,$$

by the monotony law for relative multiplication and Lemma 5.12. □

The purpose of the preceding lemma and its first dual is to specify, for an equivalence element r in a simple relation algebra $\mathfrak{A}$, the value of the relative product of $-r$ with each of three elements, namely r, $-r$, and 1. We know from Lemma 5.12 that if r is an equivalence element in $\mathfrak{A}$, then so is the relative product $-r\,;-r$. Parts (ii) and (iii) of the preceding lemma specify that $-r\,;-r$ has one of three possible values, namely 0, r, or 1, and the element $-r;1$ has one of two possible values, namely 0 or 1. Take r to be 1' in parts (ii) and (iii) of the lemma to arrive at the following corollary.

Corollary 5.25. *In a simple relation algebra, if* $0' \neq 0$, *then*

$$0' \mathbin{;} 0' = 1' \qquad \textit{or} \qquad 0' \mathbin{;} 0' = 1,$$

and $0' \mathbin{;} 1 = 1 \mathbin{;} 0' = 1$.

5.4 Right- and left-ideal elements

In discussions about binary relations, it is frequently necessary to speak about sets. For example, one may want to talk about the domain or range of a relation. How does one do this when the objects under discussion are all supposed to represent binary relations? The key is to identify a subset X of a universe of discourse U with a specific (binary) relation on U. There are two natural ways of proceeding. The first is to identified X with the relation $X \times U$ (or with the relation $U \times X$), while the second is to identified X with the subidentity relation id_X. Each approach has its advantages and disadvantages. One advantage of the first approach is that the relations representing sets are closely connected with ideals in relation algebras. This connection is very important and will be explored in depth later on.

An element r is defined to be a *right-ideal element* if $r = r \mathbin{;} 1$, and a *left-ideal element* if $r = 1 \mathbin{;} r$. The names come from the fact that these elements play a special role in determining what are sometimes called right and left ideals. The names *domain element* and *range element* respectively are sometimes also used. In a proper relation algebra on a set U, right- and left-ideal elements are relations R that can be written in the form

$$R = X \times U \qquad \text{and} \qquad R = U \times X$$

respectively, for some subset X of U. These relations may be thought of as vertical and horizontal strips respectively in the Cartesian plane determined by $U \times U$ (see Figure 5.3).

Before studying the laws that govern right-ideal elements, it is helpful to formulate a few general laws about elements of the form $r \mathbin{;} 1$. The first is a quite useful form of the De Morgan-Tarski laws that applies to certain right-ideal elements. We note in passing that the first dual of a law about right-ideal elements is a corresponding law about left-ideal elements.

Lemma 5.26. $[(r \mathbin{;} s) \cdot t] \mathbin{;} 1 = [(t \mathbin{;} s^{\smile}) \cdot r] \mathbin{;} 1$.

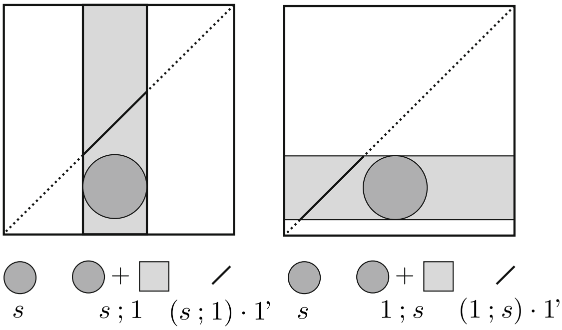


Fig. 5.3 The domain and range of an element s.

Proof. Apply Corollary 4.20 and the monotony law for relative multiplication to obtain

$$(r\,;s)\cdot t \le [(t\,;s^{\smile})\cdot r]\,;s \le [(t\,;s^{\smile})\cdot r]\,;1.$$

Form the relative product of the first and last terms with 1 on the right, and use the monotony law for relative multiplication and Lemma 4.5(iv) to arrive at

$$[(r\,;s)\cdot t]\,;1 \le [(t\,;s^{\smile})\cdot r]\,;1\,;1 = [(t\,;s^{\smile})\cdot r]\,;1. \tag{1}$$

The inequality of the first and last terms in (1) holds for all elements r, s, and t. Replace these elements with t, $s^{\smile}$, and r respectively, and use the first involution law to obtain

$$[(t\,;s^{\smile})\cdot r]\,;1 \le [(r\,;s^{\smile\smile})\cdot t]\,;1 = [(r\,;s)\cdot t]\,;1. \tag{2}$$

Together, (1) and (2) yield the desired conclusion. □

Corollary 5.27. (i) $(r\,;1)\cdot 1' = (r\,;r^{\smile})\cdot 1'$.
(ii) $[(r\,;s)\cdot 1']\,;1 = (r\cdot s^{\smile})\,;1$.
(iii) $[(r\,;1)\cdot 1']\,;1 = r\,;1$.

Proof. To prove (i), replace s and t in Lemma 5.26 with $r^{\smile}$ and $1'$ respectively to obtain

$$[(r\,;r^{\smile})\cdot 1']\,;1 = [(1'\,;r^{\smile\smile})\cdot r]\,;1. \tag{1}$$

Since $1'\,;r^{\smile\smile} = r$, by the identity law for relative multiplication and first involution law, the equality in (1) reduces to

$$[(r\,;r^\smile)\cdot 1']\,;1 = r\,;1. \tag{2}$$

Form the product of both sides of this equation with 1', and use Boolean algebra, Lemma 5.20(ii) (with $(r\,;r^\smile)\cdot 1'$ and 1' in place of r and s respectively), and (2) to arrive at

$$(r\,;r^\smile)\cdot 1' = (r\,;r^\smile)\cdot 1'\cdot 1' = ([(r\,;r^\smile)\cdot 1']\,;1)\cdot 1' = (r\,;1)\cdot 1'.$$

To prove (ii), replace t in Lemma 5.26 with 1', and use the identity law for relative multiplication and Boolean algebra. To prove (iii), replace s in (ii) with 1, and use the fact that $1^\smile = 1$, by Lemma 4.1(vi). □

We turn now to the study of right-ideal elements, and begin with some characterizations of these elements.

Lemma 5.28. *The following conditions on an element r are equivalent.*

(i) *r is a right-ideal element.*
(ii) *$r = s\,;1$ for some element s.*
(iii) *$r = x\,;1$ for some subidentity element x.*
(iv) *$r = [(r\,;1)\cdot 1']\,;1$.*
(v) *$r\,;s \leq r$ for every element s.*
(vi) *$r = r \mathbin{+\!\!\!,} 0$.*
(vii) *$r \leq r \mathbin{+\!\!\!,} s$ for every element s.*

Proof. The implication from (iv) to (iii) is trivial, as is the implication from (iii) to (ii). The implication from (ii) to (i) follows from Lemma 4.5(iv): if (ii) holds, then

$$r\,;1 = s\,;1\,;1 = s\,;1 = r.$$

The implication from (i) to (iv) follows immediately from Corollary 5.27(iii) and the definition of a right-ideal element. Thus, (i)–(iv) are all equivalent.

The equivalence of (i) and (v) is easy to check. If (v) holds, then take s to be 1 to obtain $r\,;1 \leq r$. The reverse inequality is just Lemma 4.5(iii), so (i) holds. On the other hand, if (i) holds, then $r = r\,;1 \geq r\,;s$, by the definition of a right-ideal element and the monotony law for relative multiplication, so (v) holds.

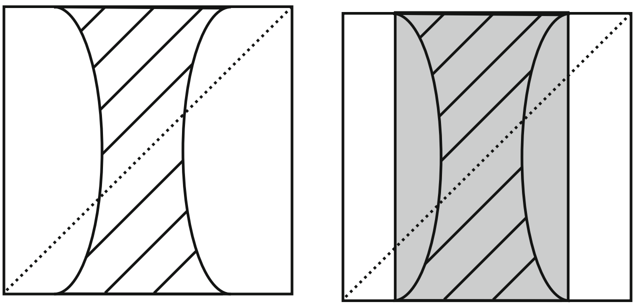
The equivalence of (i) and (vi) is a consequence of Corollary 4.31: if (i) holds, then

$$r \mathbin{\underset{,}{+}} 0 = r \mathbin{;} 1 \mathbin{\underset{,}{+}} 0 = r \mathbin{;} 1 = r,$$

and if (vi) holds, then

$$r \mathbin{;} 1 = (r \mathbin{\underset{,}{+}} 0) \mathbin{;} 1 = r \mathbin{\underset{,}{+}} 0 = r.$$

The implication from (vi) to (vii) follows from Lemma 4.7(vii), the monotony law for relative addition. On the other hand, if (vii) holds then in particular $r \le r \mathbin{\underset{,}{+}} 0$. The reverse inequality holds in general, by Lemma 4.7(viii), so we obtain (vi). □



S $\qquad$ $S \,|(U \times U)$

Fig. 5.4 A relation S and its outer cylindrification $S\,|(U \times U)$.

The equivalence of (i) and (ii) in the preceding lemma implies that there is a polynomial whose range is precisely the set of right-ideal elements in a relation algebra $\mathfrak{A}$, namely the unary operation ψ defined on $\mathfrak{A}$ by

$$\psi(s) = s \mathbin{;} 1$$

for s in $\mathfrak{A}$. This operation is distributive in the sense that

$$\psi(r + s) = \psi(r) + \psi(s)$$

for all r and s in $\mathfrak{A}$, by the distributive law for relative multiplication, so it is an operator on $\mathfrak{A}$ in the sense of Section 2.2. In particular, it is monotone, by Lemma 2.3. Moreover, the fixed points of ψ—that is to say, the elements r such that $\psi(r) = r$—are exactly the right-ideal elements in $\mathfrak{A}$, by the definition of a right-ideal element. In fact, ψ maps each element s in $\mathfrak{A}$ to the smallest right-ideal element that is above s. In more detail,

$$s \le s\,;1 = \psi(s),$$

by Lemma 4.5(iii), and if r is a right-ideal element that is above s, then

$$\psi(s) \le \psi(r) = r,$$

by the properties of ψ described above. The image $\psi(s)$ is sometimes called the *outer cylindrification* of s, or simply the right-ideal element *generated* by s. The reason is that for a relation S in a proper relation algebra on a set U, the operation ψ maps S to the smallest vertical strip, or vertical cylinder, that includes S (see Figure 5.4). Another way of thinking about ψ is that it is a geometric analogue of the operation of existential quantification in logic. Indeed, a pair of elements (α, β) belongs to the relation

$$\psi(S) = S\,|(U \times U)$$

if and only if there exists an element γ such that (α, γ) belongs to S, by the definition of relational composition.

Part (vi) of the preceding lemma says the second dual of the notion of a right-ideal element gives nothing new: it is equivalent to the definition of a right-ideal element. On the other hand, the first dual of the notion of a right-ideal element is the notion of a left-ideal element, and these two notions are clearly not equivalent.

It is often useful, but not essential, to use the form in part (iii) of the lemma when establishing laws about right-ideal elements. The reason is that with the help of part (iii), more explicit forms of the laws can be given. The next few lemmas furnish some concrete examples of this. In the statements and proofs of these lemmas, the elements x and y are always assumed to be subidentity elements.

A right-ideal element r may be written in the form $r = s\,;1$ in many different ways, that is to say, r may be generated as a right-ideal element by many different elements s. However, there is only one subidentity element that generates r as a right-ideal element.

Lemma 5.29. *Suppose* $r = x\,;1$ *and* $s = y\,;1$.

(i) $r \le s$ *if and only if* $x \le y$.
(ii) $r = s$ *if and only if* $x = y$.

Proof. The implication from right to left in (i) follows from the monotony law for relative multiplication. For the reverse implication, observe that

$$r \cdot x = (x\,;1) \cdot x = x \qquad \text{and} \qquad s \cdot x = (y\,;1) \cdot x = y \cdot x, \tag{1}$$

by the hypotheses of the lemma, together with (iii) and (ii) from Lemma 5.20. If $r \leq s$, then $r \cdot x \leq s \cdot x$, by Boolean algebra, and therefore $x \leq y \cdot x$, by (1). This last inequality implies that $x \leq y$, which completes the proof of (i). Part (ii) is an immediate consequence of (i). □

The next two lemmas state some of the basic closure properties of the set of right-ideal elements. The first lemma concerns the closure of this set under the Boolean operations of the given relation algebra.

Lemma 5.30. (i) *The distinguished constants* 0 *and* 1 *are right-ideal elements.*

(ii) *The sum of a set of right-ideal elements, if it exists, is a right-ideal element. In fact, if* X *is a set of subidentity elements, then* $\sum X$ *exists if and only if* $\sum\{x\,;1 : x \in X\}$ *exists, and if one of these sums exists, then*

$$(\textstyle\sum X)\,;1 = \sum\{x\,;1 : x \in X\}.$$

In particular, if $r = x\,;1$ *and* $s = y\,;1$, *then* $r + s = (x + y)\,;1$.

(iii) *The product of a set of right-ideal elements, if it exists, is a right-ideal element. In fact, if* X *is a set of subidentity elements, then* $\prod X$ *exists if and only if* $\prod\{x\,;1 : x \in X\}$ *exists, and if one of these products exists, then*

$$(\textstyle\prod X)\,;1 = \prod\{x\,;1 : x \in X\}.$$

In particular, if $r = x\,;1$ *and* $s = y\,;1$, *then* $r \cdot s = (x \cdot y)\,;1$.

(iv) *If* r *is a right-ideal element, then so is* $-r$. *In fact, if* $r = x\,;1$, *then* $-r = (1\text{'} - x)\,;1$.

Proof. Part (i) follows from Lemma 4.5(iv) and the first dual of Corollary 4.17. In order to prove (ii), observe first that every set Y of right-ideal elements may be written in the form

$$Y = \{x\,;1 : x \in X\} \tag{1}$$

for some set X of subidentity elements, by Lemma 5.28. If $\sum Y$ exists, then

$$\begin{aligned}(\textstyle\sum Y) \cdot 1\text{'} &= (\textstyle\sum\{x\,;1 : x \in X\}) \cdot 1\text{'}\\ &= \textstyle\sum\{(x\,;1) \cdot 1\text{'} : x \in X\} = \sum\{x : x \in X\},\end{aligned}$$

by (1), Boolean algebra, and Lemma 5.20(ii) (with x and 1' in place of r and s respectively), together with the assumption that x is below 1'. Consequently, $\sum X$ exists, and

$$(\textstyle\sum X)\,;1=\sum\{x\,;1:x\in X\}=\sum Y, \tag{2}$$

by the complete distributivity of relative multiplication and (1). On the other hand, if $\sum X$ exists, then $\sum Y$ exists and (2) holds, by the complete distributivity of relative multiplication and the computation in (2).

We next establish the special case of (iii) when

$$r=x\,;1 \qquad \text{and} \qquad s=y\,;1. \tag{3}$$

Use (3), the second modular law in Lemma 5.15 (with 1, y, and x in place of r, s, and t respectively), and Lemma 5.20(ii) (with x and y in place of r and s respectively) to obtain

$$r\cdot s=(x\,;1)\cdot(y\,;1)=[(x\,;1)\cdot y]\,;1=(x\cdot y)\,;1, \tag{4}$$

as desired. (Lemma 5.15 is applicable because 1 is an equivalence element, by Lemma 5.9(i).)

Part (iv) of the lemma is now easy to prove. If

$$r=x\,;1 \qquad \text{and} \qquad s=(1'-x)\,;1, \tag{5}$$

then

$$r+s=(x\,;1)+(1'-x)\,;1=[x+(1'-x)]\,;1=1'\,;1=1,$$

by (5), part (ii) of the lemma, Boolean algebra, and the identity law for relative multiplication; and

$$r\cdot s=(x\,;1)\cdot(1'-x)\,;1=[x\cdot(1'-x)]\,;1=0\,;1=0,$$

by (5), (4) (with $1'-x$ in place of y), Boolean algebra, and the first dual of Corollary 4.17. It follows from these equations and Boolean algebra that $s=-r$.

Turn finally to the proof of (iii). Let Y be a set of right-ideal elements, and take X to be a set of subidentity elements such that (1) holds. Write

$$Z=\{1'-x:x\in X\}, \tag{6}$$

and observe that $\prod X$ exists if and only if $\sum Z$ exists. In fact,

$$1\text{'} - \prod X = \sum Z \qquad \text{and} \qquad 1\text{'} - \sum Z = \prod X, \tag{7}$$

by Boolean algebra. To prove (iii), assume first that $\prod X$ exists. In this case,

$$\begin{aligned} -[(\textstyle\prod X) ; 1] &= (1\text{'} - \textstyle\prod X) ; 1 = (\textstyle\sum Z) ; 1 \\ &= \textstyle\sum\{(1\text{'} - x) ; 1 : x \in X\} = \textstyle\sum\{-(x ; 1) : x \in X\}. \end{aligned} \tag{8}$$

The first and last equalities use (iv), while the second equality uses (7) and the third uses (ii) and (6). The complement of the last term in (8) coincides with $\prod Y$, by (1) and Boolean algebra, so it may be concluded from (8) that $\prod Y$ exists and

$$-[(\textstyle\prod X) ; 1] = -(\textstyle\prod Y).$$

Consequently,

$$(\textstyle\prod X) ; 1 = \textstyle\prod Y = \textstyle\prod\{x ; 1 : x \in X\}. \tag{9}$$

Assume now that $\prod Y$ exists. Observe that

$$\begin{aligned} (\textstyle\prod Y) \cdot 1\text{'} &= (\textstyle\prod\{x ; 1 : x \in X\}) \cdot 1\text{'} \\ &= \textstyle\prod\{(x ; 1) \cdot 1\text{'} : x \in X\} = \textstyle\prod\{x : x \in X\}, \end{aligned}$$

by (1), Boolean algebra, and Lemma 5.20(ii) (with x and 1' in place of r and s respectively), together with the assumption that the elements in X are subidentity elements. From this it follows that $\prod X$ exists, and therefore (9) holds, by the argument in the preceding paragraph. This completes the proof of (iii). □

The notion of an ideal will be discussed at length in Chapter 8, but it may be useful at this point to say a few words about right-ideals. A *right-ideal* in a relation algebra $\mathfrak{A}$ is a subset M of $\mathfrak{A}$ that contains zero, is closed under addition, and contains $r \cdot s$ and $r ; s$ whenever r is in M and s in $\mathfrak{A}$. It is readily verified that for any element r in $\mathfrak{A}$, the set of elements below r is a right-ideal if and only if r is a right-ideal element. This connection is the motivation behind the name of these particular elements.

The outer cylindrification operation defined before Lemma 5.28 has a corresponding second dual, which is the operation ϑ defined for every s in $\mathfrak{A}$ by

$$\vartheta(s) = s \mathbin{+\!\!\!,} 0 = -(-s\,;1).$$

This operation is distributive over multiplication in the sense that

$$\vartheta(r \cdot s) = \vartheta(r) \cdot \vartheta(s)$$

for all r and s in $\mathfrak{A}$, by the distributive law for relative addition over multiplication, and ϑ is monotone, by the monotony law for relative addition. The range of ϑ consists of right-ideal elements, by Lemma 5.30(iv). Moreover, ϑ maps every right-ideal element r to itself, since

$$\vartheta(r) = r \mathbin{+\!\!\!,} 0 = r,$$

by the definition of ϑ and Lemma 5.28(vi). Combine these two observations to conclude that the fixed points of ϑ are precisely the right-ideal elements in $\mathfrak{A}$. In fact, ϑ maps each element s to the largest right-ideal element that is below s. In more detail,

$$\vartheta(s) = s \mathbin{+\!\!\!,} 0 \leq s,$$

by the definition of ϑ and Lemma 4.7(viii), and if r is a right-ideal element that is below s, then

$$r = \vartheta(r) \leq \vartheta(s),$$

by the properties of ϑ described above. The image $\vartheta(s)$ is sometimes called the *inner cylindrification* of s. The reason is that for a relation S in a proper relation algebra on a set U, the operation ϑ maps S to the largest vertical strip, or vertical cylinder, that is entirely included in S (see Figure 5.5). Another way of thinking about ψ is that it is a geometric analogue of the operation of universal quantification in logic. Indeed, a pair of elements (α, β) from U belongs to the relation

$$\vartheta(S) = S \dagger \varnothing$$

if and only if for all elements γ in U, the pair (α, γ) belongs to S, by the definition of relational addition.

Lemma 5.30 implies that the set B of right-ideal elements in a relation algebra $\mathfrak{A}$ is a Boolean algebra under the Boolean operations of $\mathfrak{A}$, and actually a (Boolean) subalgebra of the Boolean part of $\mathfrak{A}$. It is called the *Boolean algebra of right-ideal elements* in $\mathfrak{A}$. In fact, B is a *strongly regular subalgebra* of the Boolean part of $\mathfrak{A}$ in the sense that the supremum of a subset of B exists in B if and only if it exists in $\mathfrak{A}$, and when the two suprema exist, they are equal.

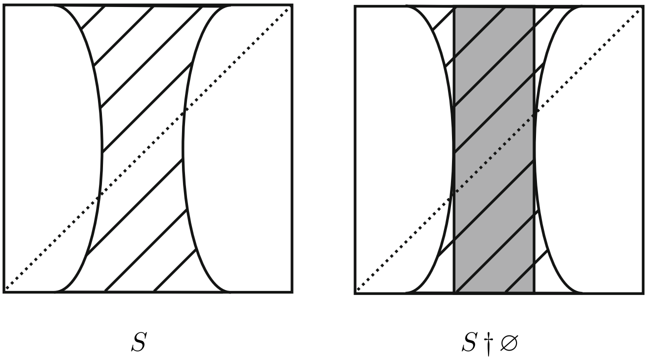


Fig. 5.5 A relation S and its inner cylindrification $S \dagger \varnothing$.

Lemma 5.31. *A set of right-ideal elements in a relation algebra* $\mathfrak{A}$ *has a supremum in* $\mathfrak{A}$ *if and only if it has a supremum in the Boolean algebra of right-ideal elements of* $\mathfrak{A}$, *and when these suprema exist, they are equal.*

Proof. Let X be a set of right-ideal elements in $\mathfrak{A}$. If X has a supremum r in $\mathfrak{A}$, then r is a right-ideal element, by Lemma 5.30(ii), and therefore r belongs to the Boolean algebra B of right-ideal elements in $\mathfrak{A}$. Clearly, r must also be the supremum of X in B.

Assume now that X has a supremum r in B, with the goal of showing that r is the supremum of X in $\mathfrak{A}$. Obviously, r is an upper bound of X in $\mathfrak{A}$. Consider now any upper bound s of X in $\mathfrak{A}$. Thus, $t \leq s$ for each t in X. The set X consists of right-ideal elements, and the inner cylindrification operation ϑ mentioned before the lemma is monotone, fixes right-ideal elements, and maps s to the largest right-ideal element below below s, so

$$t = \vartheta(t) \leq \vartheta(s) \leq s$$

for each t in X. In particular $\vartheta(s)$ is a right-ideal element that is an upper bound for X in $\mathfrak{A}$, and therefore also an upper bound for X in B, because $\vartheta(s)$ belongs to B. The element r is assumed to be the least upper bound of X in B, so

$$r \leq \vartheta(s) \leq s.$$

Conclusion: r is the least upper bound of X in $\mathfrak{A}$. □

It follows from the next lemma that the set B of right-ideal elements is closed under relative multiplication and relative addition; but in

general B is not closed under converse and it does not contain the identity element or the diversity element, so B is not a subuniverse of $\mathfrak{A}$.

Lemma 5.32. (i) *If r is a right-ideal element, then $s\,;r$ is a right ideal element for every element s.*

(ii) *If r is a right-ideal element, then $s \dagger r$ is a right-ideal element for every element s.*

(iii) *If r is a right-ideal element, then $r^{\smile}$ is a left-ideal element. In fact, if $r = x\,;1$, then $r^{\smile} = 1\,;x$.*

Proof. Assume r is a right-ideal element and s an arbitrary element. The definition of a right-ideal element implies that

$$s\,;r\,;1 = s\,;r,$$

so (i) holds. To prove (ii), observe that $-r$ is also a right-ideal element, by Lemma 5.30(iv), and therefore so is $-s\,;-r$, by (i). Another application of Lemma 5.30(iv) leads to the conclusion that $-(-s\,;-r)$ is a right-ideal element. Since $s \dagger r$ coincides with this last term, by definition, we arrive at (ii). Part (iii) follows from the second involution law and Lemmas 4.1(vi) and 5.20(i). □

There is a strong connection between the atoms in the Boolean algebra of right-ideal elements of a relation algebra $\mathfrak{A}$ and the *subidentity atoms* in $\mathfrak{A}$, that is to say, the atoms in $\mathfrak{A}$ that are below the identity element.

Lemma 5.33. *Let r be an element in a relation algebra $\mathfrak{A}$.*

(i) *If r is an atom in $\mathfrak{A}$, then $r\,;1$ is an atom in the Boolean algebra of right-ideal elements in $\mathfrak{A}$.*

(ii) *$r\,;1$ is an atom in the Boolean algebra of right-ideal elements if and only if $(r\,;1)\cdot 1'$ is an atom in $\mathfrak{A}$.*

Proof. To prove (i), assume that r is an atom in $\mathfrak{A}$, and consider an arbitrary right-ideal element s. Either $r \le s$ or $r \le -s$, by the assumption on r, so either

$$r\,;1 \le s\,;1 = s \qquad \text{or} \qquad r\,;1 \le -s\,;1 = -s, \tag{1}$$

by the monotony law for relative multiplication, the assumption that s is a right-ideal element, and Lemma 5.30(iv). Since $r\,;1$ is not zero, by

Lemma 4.5(iii), it follows from (1) that $r\,;1$ is an atom in the Boolean algebra of right-ideal elements.

To prove (ii), write $x = (r\,;1) \cdot 1\text{'}$, and observe that $r\,;1 = x\,;1$, by Corollary 5.27(iii). If x is an atom in $\mathfrak{A}$, then $x\,;1$ in a atom in the Boolean algebra of right-ideal elements, by part (i). On the other hand, if $x\,;1$ is an atom in the Boolean algebra of right-ideal elements, then $x \neq 0$, by the first dual of Corollary 4.17, and for every subidentity element y we either have

$$x\,;1 \leq y\,;1 \qquad \text{or} \qquad x\,;1 \leq -(y\,;1) = (1\text{'} - y)\,;1.$$

In the first case, $x \leq y$, and in the second case, $x \leq 1\text{'} - y$, by Lemma 5.29(i). Consequently, for any element s, either

$$x \leq s \cdot 1\text{'} \leq s \qquad \text{or} \qquad x \leq 1\text{'} - (s \cdot 1\text{'}) \leq -s,$$

so x is an atom in $\mathfrak{A}$. □

The next lemma says that right-ideal elements are idempotent with respect to the operations of relative addition and multiplication.

Lemma 5.34. *If r is a right-ideal element, then*

$$r\,;r = r \qquad \textit{and} \qquad r \mathbin{+\!\!\!,} r = r.$$

Proof. Assume r is a right-ideal element. We have $r\,;r \leq r\,;1 = r$, by the monotony law for relative multiplication and the definition of a right-ideal element; and

$$r \leq r\,;r^{\smile}\,;r \leq r\,;1\,;r = r\,;r,$$

by Corollary 4.22, the monotony law for relative multiplication, and the definition of a right-ideal element; so $r\,;r = r$. This proves the first law.

To derive the second law, observe that $-r$ is a right-ideal element, by Lemma 5.30(iv), and therefore $-r\,;-r = -r$, by the first law. Consequently,

$$r \mathbin{+\!\!\!,} r = -(-r\,;-r) = -(-r) = r.$$

The first and last equalities use the definition of relative addition and Boolean algebra. □

There are two modular laws that are valid for right-ideal elements, and each of these laws actually characterizes right-ideal elements. The first law concerns the modularity of multiplication over relative multiplication.

Lemma 5.35. *An element r is a right-ideal element if and only if*

$$r \cdot (s \mathbin{;} t) = (r \cdot s) \mathbin{;} t$$

for all elements s and t.

Proof. If r is a right-ideal element, and s and t arbitrary elements, then

$$r \mathbin{;} t \leq r \mathbin{;} 1 = r \qquad \text{and} \qquad r \mathbin{;} t^{\smile} \leq r \mathbin{;} 1 = r,$$

by the monotony law for relative multiplication and the definition of a right-ideal element, so

$$r \cdot (s \mathbin{;} t) = (r \cdot s) \mathbin{;} t, \tag{1}$$

by Corollary 4.33. On the other hand, if r satisfies the law in (1) for all elements s and t, then take s and t to be 1, and use also Boolean algebra and Lemma 4.5(iv), to arrive at

$$r = r \cdot 1 = r \cdot (1 \mathbin{;} 1) = (r \cdot 1) \mathbin{;} 1 = r \mathbin{;} 1.$$

Thus, r is a right-ideal element. □

It follows from the preceding modular law that for an arbitrary element r, the element $(r \mathbin{;} 1) \cdot 1'$ acts as a left-hand identity element for r with respect to the operation of relative multiplication.

Corollary 5.36. $[(r \mathbin{;} 1) \cdot 1'] \mathbin{;} r = r$.

Proof. We have

$$r = (r \mathbin{;} 1) \cdot r = (r \mathbin{;} 1) \cdot (1' \mathbin{;} r) = [(r \mathbin{;} 1) \cdot 1'] \mathbin{;} r,$$

by Boolean algebra and Lemmas 4.5(iii), 4.4(ii), and 5.35 (with $r;1$, $1'$, and r in place of r, s, and t respectively). □

The second characterization of right-ideal elements concerns the modularity of multiplication over relative addition.

Lemma 5.37. *An element r is a right-ideal element if and only if*

$$r \cdot [s \mathbin{\underset{,}{+}} (r \cdot t)] = (r \cdot s) \mathbin{\underset{,}{+}} (r \cdot t)$$

for all elements s and t.

Proof. Assume first that r is a right-ideal element, and s and t are arbitrary elements. The distributive law for relative addition over multiplication (Lemma 4.7(iv), applied twice) implies that

$$\begin{aligned}(r \cdot s) \mathbin{\underset{,}{+}} (r \cdot t) &= [r \mathbin{\underset{,}{+}} (r \cdot t)] \cdot [s \mathbin{\underset{,}{+}} (r \cdot t)] \\ &= (r \mathbin{\underset{,}{+}} r) \cdot (r \mathbin{\underset{,}{+}} t) \cdot [s \mathbin{\underset{,}{+}} (r \cdot t)]. \qquad (1)\end{aligned}$$

Since

$$r \mathbin{\underset{,}{+}} r = r \leq r \mathbin{\underset{,}{+}} t,$$

by Lemmas 5.34 and 5.28(vii), it may be concluded from (1) that

$$(r \cdot s) \mathbin{\underset{,}{+}} (r \cdot t) = r \cdot [s \mathbin{\underset{,}{+}} (r \cdot t)].$$

Thus, the given modular law holds.

On the other hand, if the modular law holds for all elements s and t, then take s and t to be 1 and 0 respectively, and use also Boolean algebra and the third dual of Corollary 4.17, to arrive at

$$r = r \cdot 1 = r \cdot (1 \mathbin{\underset{,}{+}} 0) = r \cdot [1 \mathbin{\underset{,}{+}} (r \cdot 0)] = (r \cdot 1) \mathbin{\underset{,}{+}} (r \cdot 0) = r \mathbin{\underset{,}{+}} 0. \qquad (2)$$

Apply Lemma 5.28(vi) to (2) to conclude that r is a right-ideal element. □

5.5 Ideal elements

An element r in a relation algebra is defined to be an *ideal element* if $1 \mathbin{;} r \mathbin{;} 1 = r$. The name derives from the close connection that exists between elements of this form and ideals, that is to say, kernels of homomorphisms. This connection is extremely important and will be explored in some depth in Chapter 8. In the full relation algebra on an equivalence relation E, the ideal elements are just the relations R that can be written in the form

$$R = \bigcup\{V \times V : V \in X\}$$

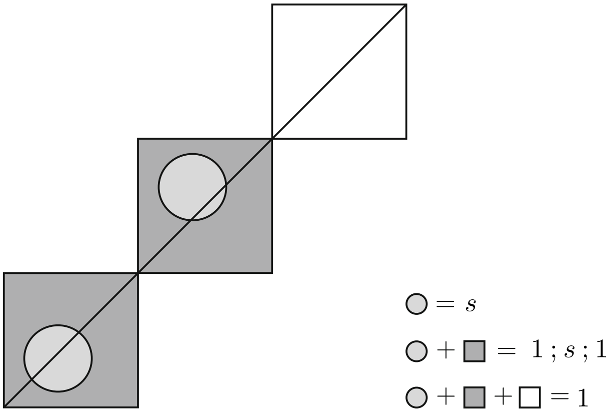


Fig. 5.6 An element s and the ideal element $1 ; s ; 1$ that s generates.

for some set X of equivalence classes of E (see Figure 5.6). In particular, if V is an equivalence class of E, then $V \times V$ is an ideal element.

Here are some useful characterizations of ideal elements.

Lemma 5.38. *The following conditions on an element r are equivalent.*

(i) *r is an ideal element.*
(ii) $r = 1 ; s ; 1$ *for some element s.*
(iii) $r = 1 ; x ; 1$ *for some subidentity element x.*
(iv) $r = 1 ; [(r ; 1) \cdot 1'] ; 1$.
(v) $r = 1 ; [(1 ; r) \cdot 1'] ; 1$.
(vi) *r is both a right- and a left-ideal element.*
(vii) $r = 0 \mathbin{+\!\!\!\!\!,}\; r \mathbin{+\!\!\!\!\!,}\; 0$.
(viii) $r = 0 \mathbin{+\!\!\!\!\!,}\; s \mathbin{+\!\!\!\!\!,}\; 0$ *for some element s.*

Proof. The implications from (iv) to (iii) and from (v) to (iii) are trivial, as is the implication from (iii) to (ii). The implication from (ii) to (i) follows by Lemma 4.5(iv); indeed, if r satisfies (ii), then

$$1 ; r ; 1 = 1 ; 1 ; s ; 1 ; 1 = 1 ; s ; 1 = r.$$

For the implication from (i) to (vi), observe that if r is an ideal element, then

$$r = 1 ; r ; 1 = 1 ; r ; 1 ; 1 = r ; 1,$$

by Lemma 4.5(iv) and the definitions of ideal and right-ideal elements, so r is a right-ideal element. A dual argument shows that r is a left-ideal element. For the implication from (vi) to (iv), observe that if r is a right- and a left-ideal element, then

$$r = 1 ; r = 1 ; [(r ; 1) \cdot 1'] ; 1,$$

by the definition of a left-ideal element and Lemma 5.28(iv). An analogous argument shows that (vi) implies (v). Thus, (i)–(vi) are all equivalent.

The implication from (vii) to (viii) is trivial; and (viii) implies (i), by the first law in Corollary 4.31 and its first dual: if (viii) holds, then

$$1 ; r ; 1 = 1 ; (0 \dagger s \dagger 0) ; 1 = 0 \dagger s \dagger 0 = r.$$

The implication from (i) to (vii) is proved in an analogous fashion, but uses the second law in Corollary 4.31 and its first dual. Thus, (i), (vii), and (viii) are also equivalent. □

The equivalence of (i) and (ii) in the preceding lemma implies that there is a polynomial whose range is precisely the set of ideal elements in a relation algebra $\mathfrak{A}$, namely the unary operation ψ defined on $\mathfrak{A}$ by

$$\psi(s) = 1 ; s ; 1.$$

This operation is distributive, by the distributive law for relative multiplication, so it is an operator on $\mathfrak{A}$ in the sense of Section 2.2. In particular, it is monotone, by Lemma 2.3. Moreover, its fixed points—that is to say, the elements r such that $\psi(r) = r$—are exactly the ideal elements in $\mathfrak{A}$, by the definition of an ideal element. In fact, ψ maps each element s in $\mathfrak{A}$ to the smallest ideal element that is above s. In more detail,

$$s \leq 1 ; s ; 1 = \psi(s),$$

by Lemma 4.5(iii) and its first dual, and if r is an ideal element that is above s, then

$$\psi(s) \leq \psi(r) = r,$$

by the properties of ψ described above. The image $\psi(s)$ may be called the *outer ideal closure* of s, or simply the ideal element *generated* by s.

The notion of an ideal element is clearly its own first dual, that is to say, the first dual of the notion of an ideal element coincides with the notion of an ideal element. The equivalence of (i) and (vii) in the

preceding lemma implies that this is also true for the second dual, and consequently also for the third dual.

The next two lemmas give some of the basic closure properties of the set of ideal elements. The first lemma concerns the closure of this set under Boolean operations.

Lemma 5.39. (i) 0 *and* 1 *are ideal elements.*

(ii) *The sum of a set of ideal elements, if it exists, is an ideal element. In particular, if* r *and* s *are ideal elements, then so is* $r + s$.

(iii) *The product of a set of ideal elements, if it exists, is an ideal element. In particular, if* r *and* s *are ideal elements, then so is* $r \cdot s$.

(iv) *If* r *is an ideal element, then so is* $-r$.

Proof. The lemma follows directly from Lemma 5.30 and its first dual for left-ideal elements, together with the characterization of ideal elements in Lemma 5.38(vi). For example, both 0 and 1 are right-ideal elements and left-ideal elements, by Lemma 5.30(i) and its first dual, so both of them are ideal elements, by Lemma 5.38(vi). The proofs of parts (ii)–(iv) are entirely analogous. □

The outer ideal closure operation defined before Lemma 5.39 has a corresponding second dual, which is the unary operation ϑ defined for every s in $\mathfrak{A}$ by

$$\vartheta(s) = 0 \mathbin{\underset{,}{+}} s \mathbin{\underset{,}{+}} 0 = -(1 \,;\, -s \,;\, 1).$$

This operation is monotone and distributive over multiplication, by the monotony and distributive laws for relative addition. The range of ϑ consists of ideal elements, by Lemma 5.38(viii). Moreover, ϑ maps every ideal element r to itself, since

$$\vartheta(r) = 0 \mathbin{\underset{,}{+}} r \mathbin{\underset{,}{+}} 0 = r,$$

by the definition of ϑ and Lemma 5.38(vii). Combine these two observations to conclude that the fixed points of ϑ are precisely the ideal elements in $\mathfrak{A}$. In fact, ϑ maps each element s to the largest ideal element that is below s. In more detail,

$$\vartheta(s) = 0 \mathbin{\underset{,}{+}} s \mathbin{\underset{,}{+}} 0 \leq s,$$

by the definition of ϑ, together with Lemma 4.7(viii) and its first dual; and if r is an ideal element that is below s, then

$$r = \vartheta(r) \le \vartheta(s),$$

by the properties of ϑ described above. The image $\vartheta(s)$ may be called the *inner ideal closure* of s.

It follows from Lemma 5.39 that the set B of ideal elements in a relation algebra $\mathfrak{A}$ is a Boolean algebra under the Boolean operations of $\mathfrak{A}$, and actually a (Boolean) subalgebra of the Boolean part of $\mathfrak{A}$. It is called the *Boolean algebra of ideal elements* in $\mathfrak{A}$. In fact, B is a strongly regular subalgebra of the Boolean part of $\mathfrak{A}$ in the sense specified before Lemma 5.31.

Lemma 5.40. *A set of ideal elements in a relation algebra* $\mathfrak{A}$ *has a supremum in* $\mathfrak{A}$ *if and only if it has a supremum in the Boolean algebra of ideal elements of* $\mathfrak{A}$, *and when these suprema exist*, *they are equal.*

The proof is analogous to the proof of Lemma 5.31. The word "right-ideal" in that proof must be replaced everywhere by the word "ideal", the reference Lemma 5.30(ii) must be replaced by a reference to Lemma 5.39(ii), and the inner cylindrification operation must be replaced everywhere by the inner ideal closure operation. The details are left as an exercise.

The next lemma implies that the Boolean algebra of ideal elements in $\mathfrak{A}$ is also closed under the Peircean operations of $\mathfrak{A}$.

Lemma 5.41. (i) *If* r *is an ideal element*, *then* $r^{\smile} = r$, *and therefore* $r^{\smile}$ *is an ideal element.*

(ii) *If* r *and* s *are ideal elements*, *then* $r \,;\, s = r \cdot s$, *and therefore* $r \,;\, s$ *is an ideal element.*

(iii) *If* r *and* s *are ideal elements*, *then* $r \mathbin{+\!\!,} s = r + s$, *and therefore* $r \mathbin{+\!\!,} s$ *is an ideal element.*

Proof. To prove (i), assume r is an ideal element, and observe that

$$r^{\smile} \le r^{\smile} \,;\, r^{\smile\smile} \,;\, r^{\smile} = r^{\smile} \,;\, r \,;\, r^{\smile} \le 1 \,;\, r \,;\, 1 = r,$$

by Corollary 4.22 (with $r^{\smile}$ in place of r), the first involution law, the monotony law for relative multiplication, and the assumption on r. Thus, r is symmetric. Apply Lemma 5.1(ii) to conclude that $r^{\smile} = r$.

To prove (ii) and (iii), assume r and s are ideal elements, and observe that

$$r \,;\, s = r \,;\, 1 \,;\, s = (r \,;\, 1) \cdot (1 \,;\, s) = r \cdot s,$$

by Lemmas 5.38(vi) and 4.26. This gives (ii). Since $-r$ and $-s$ are also ideal elements, by Lemma 5.39(iv), we have

$$-r \mathbin{;} -s = -r \cdot -s,$$

by (ii), and therefore

$$r \mathbin{+\!\!\!,} s = -(-r \mathbin{;} -s) = -(-r \cdot -s) = r + s,$$

by the definition of relative addition and Boolean algebra. □

The proof of (i) in the preceding lemma actually shows a bit more than is claimed.

Corollary 5.42. *For every element* r,

$$r^{\smile} \leq 1 \mathbin{;} r \mathbin{;} 1 \qquad \textit{and} \qquad 1 \mathbin{;} r^{\smile} \mathbin{;} 1 = 1 \mathbin{;} r \mathbin{;} 1.$$

Lemma 5.41 also implies a stronger characterization of ideal elements than is given in parts (iv) and (v) of Lemma 5.38.

Corollary 5.43. *For* r *to be an ideal element, it is necessary and sufficient that* $r = 1 \mathbin{;} (r \cdot 1') \mathbin{;} 1$.

Proof. If r is an ideal element, then r is an equivalence element, by Lemma 5.41(i),(ii), and the definition of an equivalence element. Consequently, $r \cdot 1' = (r \mathbin{;} 1) \cdot 1'$, by Lemma 5.18(ii). Combine this observation with Lemma 5.38(iv) to conclude that $r = 1 \mathbin{;} (r \cdot 1') \mathbin{;} 1$. On the other hand, if this last equality holds, then r is an ideal element, by Lemma 5.38(ii). □

One consequence of Lemmas 5.39 and 5.41 is that the set of ideal elements in a relation algebra $\mathfrak{A}$ is closed under all of the operations of $\mathfrak{A}$. The set fails to be a subuniverse of $\mathfrak{A}$, because in general it does not contain the identity element of $\mathfrak{A}$. The set is the universe of a Boolean relation algebra under the operations of $\mathfrak{A}$, by Lemmas 5.41(ii) and 3.1; but the identity element of this Boolean relation algebra is the unit element 1 of $\mathfrak{A}$, not the identity element of $\mathfrak{A}$.

Another consequence of Lemma 5.41 is that ideal elements are equivalence elements. In particular, ideal elements satisfy the modular laws of Lemmas 5.13–5.15. As right- and left-ideal elements, they also satisfy the modular laws of Lemmas 5.35 and 5.37 and their first duals. Using either one of these observations, it can be shown that ideal elements satisfy a distributive law for multiplication over relative multiplication, and in fact ideal elements are characterized by this property.

Lemma 5.44. *An element r is an ideal element if and only if*

$$r \cdot (s \,;\, t) = (r \cdot s) \,;\, (r \cdot t)$$

for all elements s and t.

Proof. If r is an ideal element, and s and t arbitrary elements, then

$$\begin{aligned} r \cdot (s \,;\, t) = (r \cdot s) \,;\, t = [r \cdot (s \cdot r)] \,;\, t = r \cdot [(s \cdot r) \,;\, t] \\ = [(s \cdot r) \,;\, t] \cdot r = (s \cdot r) \,;\, (t \cdot r) = (r \cdot s) \,;\, (r \cdot t). \end{aligned}$$

The first and third steps use the modular law for right-ideal elements in Lemma 5.35, the fifth step uses the dual modular law for left-ideal elements, and the second, fourth, and sixth steps use Boolean algebra.

To establish the implication in the opposite direction, assume r satisfies the given distributive law for all elements s and t. Take s and t to be $-r$ and 1 respectively, and use also Boolean algebra and the first dual of Corollary 4.17, to obtain

$$r \cdot (-r \,;\, 1) = (r \cdot -r) \,;\, (r \cdot 1) = 0 \,;\, r = 0.$$

Thus, $-r \,;\, 1 \leq -r$, by Boolean algebra. The reverse inequality holds by Lemma 4.5(iii), so $-r = -r \,;\, 1$ and therefore $-r$ is a right-ideal element. Take s and t to be 1 and $-r$ respectively, and employ the same kind of argument to show that $-r = 1 \,;\, -r$ and therefore $-r$ is a left-ideal element. Use Lemma 5.38(vi) to conclude that $-r$ is an ideal element. The set of ideal elements is closed under complement, by Lemma 5.39(iv), so r must be an ideal element as well. □

Interestingly, ideal elements also satisfy a distributive law for multiplication over relative addition, and they are characterized by this property.

Lemma 5.45. *An element r is an ideal element if and only if*

$$r \cdot (s \mathbin{+\!\!\!,} t) = (r \cdot s) \mathbin{+\!\!\!,} (r \cdot t)$$

for all elements s and t.

Proof. Assume first that r is an ideal element, and s and t arbitrary elements. Apply the left-hand distributive law for relative addition over multiplication (with $r \cdot s$ and r in place of r and s respectively), and

then apply twice the right-hand distributive law for relative addition over multiplication, to obtain

$$\begin{aligned}(r \cdot s) \dagger (r \cdot t) &= [(r \cdot s) \dagger r] \cdot [(r \cdot s) \dagger t] \\ &= [(r \dagger r) \cdot (s \dagger r)] \cdot [(r \dagger t) \cdot (s \dagger t)]. \qquad (1)\end{aligned}$$

Since r is an ideal element and therefore a right- and left-ideal element, by Lemma 5.38(vi), we have

$$r = r \dagger r, \qquad r \le r \dagger t, \qquad \text{and} \qquad r \le s \dagger r, \qquad (2)$$

by Lemma 5.34 and by Lemma 5.28(vii) and its first dual (for left-ideal elements). In view of (2), the final term in (1) reduces to $r \cdot (s \dagger t)$, and this immediately yields the desired distributive law.

To establish the reverse implication, assume that r satisfies the given distributive law for all elements s and t. Apply the distributive law with 0 and 1 in place of s and t respectively, and use also Boolean algebra and the equation $0 \dagger 1 = 1$ (which holds by the second dual of Corollary 4.17) to obtain

$$r = r \cdot 1 = r \cdot (0 \dagger 1) = (r \cdot 0) \dagger (r \cdot 1) = 0 \dagger r.$$

Thus, r is a left-ideal element, by the first dual of Lemma 5.28(vi). Apply the distributive law with 1 and 0 in place of s and t respectively, and argue in an analogous fashion, to obtain $r = r \dagger 0$, so that r is a right-ideal element. Use Lemma 5.38(vi) to conclude that r is an ideal element. □

We close with a simple lemma that is quite useful.

Lemma 5.46. *If r is an ideal element, then for every element s,*

$$r \cdot s = 0 \qquad \textit{if and only if} \qquad r \cdot (1 \,;\, s \,;\, 1) = 0.$$

Proof. Use the De Morgan-Tarski laws twice and Lemma 4.1(vi) to obtain

$$\begin{aligned} r \cdot (1 \,;\, s \,;\, 1) = 0 \qquad &\text{if and only if} \qquad (1 \,;\, r) \cdot (s \,;\, 1) = 0 \\ &\text{if and only if} \qquad (1 \,;\, r \,;\, 1) \cdot s = 0. \end{aligned}$$

Since r is an ideal element, it coincides with $1 \,;\, r \,;\, 1$, and we arrive at the desired conclusion. □

5.6 Domains and ranges

As was mentioned at the beginning of Section 5.4, an alternative approach to identifying a set X with the binary relation $X \times U$ is to identify X with the subidentity relation id_X. This approach leads to the following natural definition: the *domain* and *range* of an element r are defined to be the subidentity elements

$$\text{domain } r = (r\,;1)\cdot 1' \qquad \text{and} \qquad \text{range } r = (1\,;r)\cdot 1'$$

respectively. In a set relation algebra, the domain of a relation R in the above sense is the set of pairs (α, α) such that α belongs to the domain of R in the standard sense of this word, and analogously for the range—see Figure 5.3 at the beginning of Section 5.4. The *field* of an element is defined to be the sum of its domain and range. In particular, in a set relation algebra, the field of a relation R is the set of pairs (α, α) such that α belongs either to the domain or the range of R in the standard sense of the word.

The laws in Lemma 5.18 may be viewed as statements about the field of an equivalence element r. For instance, part (ii) of the lemma and its first dual together say that

$$\text{domain } r = \text{range } r = \text{field } r = r\cdot 1',$$

while part (i) and its first dual together say that the field of r acts as an identity element for r with respect to the operation of relative multiplication.

We begin with a characterization of when two elements have the same domain.

Lemma 5.47. domain $r =$ domain s *if and only if* $r\,;1 = s\,;1$.

Proof. If $r\,;1 = s\,;1$, then obviously

$$(r\,;1)\cdot 1' = (s\,;1)\cdot 1'. \tag{1}$$

To prove the implication in the opposite direction, suppose that (1) holds. Form the relative product of both sides of this equation with 1 on the right, to get

$$[(r\,;1)\cdot 1']\,;1 = [(s\,;1)\cdot 1']\,;1.$$

Apply Corollary 5.27(iii) to conclude that $r\,;1 = s\,;1$. □

The next two lemmas contain some of the important laws about domains and ranges.

Lemma 5.48. *Suppose x is the domain, and y the range, of an element r.*

(i) $x = (r ; r^{\smile}) \cdot 1'$ *and* $y = (r^{\smile} ; r) \cdot 1'$.
(ii) $x ; r = r ; y = r$.
(iii) $x ; 1 = r ; 1$ *and* $1 ; y = 1 ; r$.
(iv) $r \leq x ; 1 ; y$.
(v) *If r is an atom, then so are x and y.*
(vi) *If r is below an equivalence element s, then*

$$x = (r ; s) \cdot (s \cdot 1') \quad \textit{and} \quad y = (s ; r) \cdot (s \cdot 1').$$

Proof. Parts (i) and (iii) follow respectively from parts (i) and (iii) of Corollary 5.27 and its first dual, and part (ii) follows from Corollary 5.36 and its first dual. For part (iv), observe that r is below $r ; 1$ and $1 ; r$, by Lemma 4.5(iii) and its first dual, so

$$r \leq (r ; 1) \cdot (1 ; r) = (x ; 1) \cdot (1 ; y) = x ; 1 ; y,$$

by part (iii) and Lemma 4.26.

Part (v) is a consequence of Lemma 5.33 and its first dual. In more detail, if r is an atom in a relation algebra, then $r ; 1$ is an atom in the Boolean algebra of right-ideal elements, by (i) of the lemma, and therefore x is an atom in the relation algebra, by part (ii) of the lemma. A dual argument shows that y is an atom.

Finally, part (vi) is a consequence of the modular laws for equivalence elements. If s is an equivalence element that is above r, then

$$(r ; 1) \cdot s = r ; (1 \cdot s) = r ; s, \tag{1}$$

by the first dual of Lemma 5.13 (with s, 1, and r in place of r, s, and t respectively) and Boolean algebra. The element x is below s, because

$$x = (r ; 1) \cdot 1' \leq (s ; 1) \cdot 1' = s \cdot 1', \tag{2}$$

by the definition of x, the monotony law for relative multiplication, and Lemma 5.18(ii). Combine (1) and (2), and use Boolean algebra and the definition of x, to arrive at

$$x = x \cdot s = [(r ; 1) \cdot 1'] \cdot s = [(r ; 1) \cdot s] \cdot (s \cdot 1') = (r ; s) \cdot (s \cdot 1').$$

A similar argument, using Lemma 5.13 instead of its first dual, leads to the second conclusion of (vi). □

Part (i) of the preceding lemma gives an alternative way of defining the domain and range of an element r. Part (vi) says that if r is below an equivalence element s, then the unit 1 and the identity element 1' may respectively be replaced by s and its field $s \cdot 1'$ in the definition of the domain and range of r. Part (ii) says that the domain and range of r act respectively as left-hand and right-hand identity elements for r with respect to the operation of relative multiplication. Actually, the domain and range of an element can be characterized as the smallest subidentity elements with this property, as the next lemma and its first dual show.

Lemma 5.49. *For an arbitrary element* r *and a subidentity element* x, *the following conditions are equivalent*:

(i) $x \,;\, r = r$,
(ii) $(r \,;\, 1) \cdot 1' \leq x$.

Proof. If (ii) holds, then

$$r = [(r \,;\, 1) \cdot 1'] \,;\, r \leq x \,;\, r \leq 1' \,;\, r = r,$$

by Lemma 5.48(ii), and the monotony and identity laws for relative multiplication. The first and last terms are the same, so equality must hold everywhere. In particular, $x \,;\, r = r$, so (i) holds. On the other hand, if (i) holds, then

$$r = x \,;\, r \leq x \,;\, 1,$$

and therefore

$$r \,;\, 1 \leq x \,;\, 1 \,;\, 1 = x \,;\, 1, \tag{1}$$

by the monotony law for relative multiplication and Lemma 4.5(iv). Consequently,

$$(r \,;\, 1) \cdot 1' \leq (x \,;\, 1) \cdot 1' = x,$$

by (1), Boolean algebra, and Lemma 5.20(iii) (with x in place of r). □

The next lemma gives a sharper form of Lemma 5.48(ii) in the case when x and r are atoms.

Lemma 5.50. *Suppose* x *and* y *are subidentity atoms*.

(i) *If* r *is an atom*, *then the following conditions are equivalent*:

(a) $x \,;\, r \neq 0$,

(b) $x\,;r = r$,
(c) $x = \text{domain } r$.

(ii) *If r is an atom, then the following conditions are equivalent*:

(a) $r\,;y \neq 0$,
(b) $r\,;y = r$,
(c) $y = \text{range } r$.

(iii) *If r is a non-zero element below $x\,;1\,;y$, then*

$$x = \text{domain } r \qquad \textit{and} \qquad y = \text{range } r.$$

Proof. We begin with the proof of (i). The implication from (c) to (b) follows from Lemma 5.48(ii), and the implication from (b) to (a) follows from the assumption that r is an atom and therefore not zero. To establish the implication from (a) to (b), assume that (a) holds, and observe that

$$0 < x\,;r \leq 1\text{'}\,;r = r,$$

by the monotony and identity laws for relative multiplication. Consequently, $x\,;r = r$, by the assumption that r is an atom. To establish the implication from (b) to (c), assume that (b) holds, and apply Lemma 5.49 to arrive at the inequality domain $r \leq x$. The reverse inequality holds because domain r is an atom, by Lemma 5.48(v), and x is an atom, by assumption. Thus, (c) holds. This completes the proof of (i).

Part (ii) is just the first dual of part (i). To prove part (iii), assume that r is a non-zero element below $x\,;1\,;y$. In this case $(x\,;1\,;y)\cdot r \neq 0$, so

$$(x\,;r)\cdot(1\,;y) \neq 0,$$

by the De Morgan-Tarski laws (with x, $1\,;y$, and r in place of r, s, and t respectively) and Lemma 5.20(i) (with x in place of r). In particular, $x\,;r$ is different from 0, so $x = \text{domain } r$, by part (i). The second conclusion of (iii) is the first dual of the first conclusion. □

Parts (i) and (ii) of the preceding lemma say that for atoms, the left-identity and right-identity properties given in Lemma 5.48(ii) actually characterize the domain and range of r. Part (iii) is a kind of converse for atoms of Lemma 5.48(iv).

For two relations R and S, the composition $R\,|\,S$ is empty if and only if the range of R is disjoint from the domain of S. The next lemma gives an abstract version of this property.

Lemma 5.51. $r\,;s = 0$ *if and only if* range r *and* domain s *are disjoint.*

Proof. The proof reduces to a series of equivalent statements:

$$\begin{aligned}
(\text{range } r)\cdot(\text{domain } s) = 0 \qquad &\text{if and only if} \qquad (1\,;r)\cdot 1'\cdot(s\,;1) = 0,\\
&\text{if and only if} \qquad (s\,;1\,;r)\cdot 1' = 0,\\
&\text{if and only if} \qquad [1'\,;(1\,;r)^{\smile}]\cdot s = 0,\\
&\text{if and only if} \qquad (r^{\smile}\,;1)\cdot s = 0,\\
&\text{if and only if} \qquad r\,;s = 0.
\end{aligned}$$

The first equivalence uses the definitions of domain and range, and Boolean algebra, the second uses Lemma 4.26, and third and fifth use the De Morgan-Tarski laws (and Boolean algebra). The fourth equivalence follows from the fact that

$$1'\,;(1\,;r)^{\smile} = (1\,;r)^{\smile} = r^{\smile}\,;1^{\smile} = r^{\smile}\,;1,$$

by the identity law for relative multiplication, the second involution law, and Lemma 4.1(vi). □

There are a number of laws that concern the domain and range of a relation constructed from other relations by means of standard set theoretic operations on relations. For example, the domain and range of a composite relation $R\,|\,S$ are respectively included in the domain of R and the range of S. The next lemma gives abstract versions of these various laws.

Lemma 5.52. (i) domain $0 =$ range $0 = 0$.
(ii) domain $1 =$ range $1 = 1'$.
(iii) domain $1' =$ range $1' = 1'$.
(iv) *If* $r \le s$, *then* domain $r \le$ domain s *and* range $r \le$ range s.
(v) domain $(r + s) =$ (domain r) $+$ (domain s) *and*
range $(r + s) =$ (range r) $+$ (range s).
(vi) domain $(r \cdot s) \le$ domain $r \cdot$ domain s *and*
range $(r \cdot s) \le$ range $r \cdot$ range s.
(vii) domain $(r^{\smile}) =$ range r *and* range $(r^{\smile}) =$ domain r.
(viii) domain $(r\,;s) \le$ domain r *and* range $(r\,;s) \le$ range s.

Proof. Here, as examples, are the proofs of the first laws in (v)–(viii). For (v), use the definition of domain, and the distributive laws for relative multiplication and multiplication to obtain

$$\begin{aligned}\text{domain }(r+s) &= [(r+s)\,;1]\cdot 1\text{'} = [(r\,;1)+(s\,;1)]\cdot 1\text{'}\\ &= [(r\,;1)\cdot 1\text{'}]+[(s\,;1)\cdot 1\text{'}] = \text{domain } r + \text{domain } s.\end{aligned}$$

For (vi), use the definition of domain, Boolean algebra, and part (ii) of Lemma 4.5 to obtain

$$\begin{aligned}\text{domain }(r\cdot s) &= [(r\cdot s)\,;1]\cdot 1\text{'} = [(r\cdot s)\,;(1\cdot 1)]\cdot 1\text{'}\\ &\le [(r\,;1)\cdot(s\,;1)]\cdot 1\text{'} = [(r\,;1)\cdot 1\text{'}]\cdot[(s\,;1)\cdot 1\text{'}]\\ &= \text{domain } r\cdot \text{domain } s.\end{aligned}$$

For (vii), use the definition of domain, Lemmas 4.1(vi) and 4.3, the second involution law, Lemma 4.1(ii), Lemma 5.20(i), and the definition of range to get

$$\begin{aligned}\text{domain }(r^{\smile}) &= (r^{\smile}\,;1)\cdot 1\text{'} = (r^{\smile}\,;1^{\smile})\cdot 1\text{'}^{\smile} = [(1\,;r)^{\smile}]\cdot 1\text{'}^{\smile}\\ &= [(1\,;r)\cdot 1\text{'}]^{\smile} = (1\,;r)\cdot 1\text{'} = \text{range } r.\end{aligned}$$

Finally, for (viii), use the definition of domain and the monotony law for relative multiplication to get

$$\text{domain }(r\,;s) = (r\,;s\,;1)\cdot 1\text{'} \le (r\,;1)\cdot 1\text{'} = \text{domain } r.$$

The proofs of the second parts of (v)–(viii) are the first duals of the proofs of the first parts, and the proofs of (i)–(iv) are quite easy. □

5.7 Rectangles

A set-theoretical rectangle is a relation of the form $X \times Y$, where the sides X and Y of the rectangle are subsets of some base set (see Figure 5.7). The set-theoretical perspective motivates the abstract definition: an element r in a relation algebra is defined to be a *rectangle* if $r = x\,;1\,;y$ for some subidentity elements x and y, and x and y are called the *sides* of the rectangle. Observe that every right-ideal element r is a rectangle, since $r = x\,;1 = x\,;1\,;1\text{'}$ for some subidentity element x. In particular, 0 and 1 are rectangles. Similarly, every left-ideal element is a rectangle.

There are a variety of characterizations of rectangles.

Lemma 5.53. *The following conditions on an element r are equivalent.*

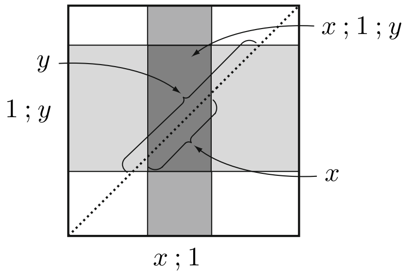


Fig. 5.7 A typical set-theoretical rectangle $x ; 1 ; y$.

(i) *r is a rectangle.*
(ii) *r is the product of a right- and a left-ideal element.*
(iii) $r = r ; 1 ; r$.
(iv) $r = s ; 1 ; s$ *for some element* s.
(v) $r = s ; 1 ; t$ *for some elements* s *and* t.
(vi) $r = [(r ; 1) \cdot 1'] ; 1 ; [(1 ; r) \cdot 1']$.

Proof. The implications from (vi) to (i), from (i) to (v), from (iii) to (iv), and from (iv) to (v) are all trivial, while the equivalence of (v) and (ii) follows from Lemma 4.26, together with Lemma 5.28(ii) and its first dual. It remains to establish the implications from (iii) to (vi), and from (v) to (iii). If (iii) holds, then

$$\begin{aligned} r = r ; 1 ; r = (r ; 1) \cdot (1 ; r) &= ([(r ; 1) \cdot 1'] ; 1) \cdot (1 ; [(1 ; r) \cdot 1']) \\ &= [(r ; 1) \cdot 1'] ; 1 ; [(1 ; r) \cdot 1'], \end{aligned}$$

by Lemma 4.26 (for the second and fourth equalities), and Corollary 5.27(iii) and its first dual, so (vi) holds.

If (v) holds for some s and t, then

$$r ; 1 = s ; 1 ; t ; 1 \leq s ; 1 \qquad \text{and} \qquad 1 ; r = 1 ; s ; 1 ; t \leq 1 ; t, \tag{1}$$

by the monotony law for relative multiplication, so

$$(r ; 1) \cdot (1 ; r) \leq (s ; 1) \cdot (1 ; t) = s ; 1 ; t = r, \tag{2}$$

by (1), Boolean algebra, Lemma 4.26, and the assumption on r. The reverse inequality—that r is below the first term in (2)—holds, by Lemma 4.5(iii) and its first dual, so

$$r = (r ; 1) \cdot (1 ; r) = r ; 1 ; r,$$

by Lemma 4.26. □

The equivalence of (i) and (iv) in the preceding lemma implies that there is a polynomial whose range is the set of rectangles in a relation algebra $\mathfrak{A}$, namely the function ψ defined on $\mathfrak{A}$ by

$$\psi(s) = s\,;1\,;s$$

for each element s.

It is often convenient to refer to a rectangle by using its sides, and we do so in the presentation below. This raises the question of whether the sides of a non-zero rectangle are uniquely determined. See Lemma 5.63 below for some remarks regarding this question.

The arithmetic and the closure properties of rectangles are, in part, somewhat complicated to formulate. For that reason, we break the statements down into a series of lemmas. In the statements and proofs of these lemmas, the elements x, y, u, and v are always assumed to be subidentity elements. The first lemma says that a product of a rectangle with an arbitrary element s is close in form to a rectangle.

Lemma 5.54. $(x\,;1\,;y)\cdot s = x\,;s\,;y$.

Proof. We have

$$(x\,;1\,;y)\cdot s = (x\,;1)\cdot(1\,;y)\cdot s = (x\,;1)\cdot(s\,;y) = x\,;s\,;y,$$

by Lemma 4.26, the first dual of Lemma 5.21 (with y in place of r), and Lemma 5.21 itself (with x and $s\,;y$ in place of r and s). □

A sum of rectangles is in general not a rectangle, but a product of rectangles is a rectangle. The precise formulation of this assertion is somewhat delicate in the case of infinitely many rectangles.

Lemma 5.55. *If* $(x_i : i \in I)$ *and* $(y_i : i \in I)$ *are systems of subidentity elements such that the products* $\prod_i x_i$ *and* $\prod_i y_i$ *exist, then the product of the system of rectangles* $(x_i\,;1\,;y_i : i \in I)$ *exists, and*

$$(\textstyle\prod_i x_i)\,;1\,;(\prod_i y_i) = \prod_i(x_i\,;1\,;y_i).$$

Proof. Assume that the products $\prod_i x_i$ and $\prod_i y_i$ exist. The products

$$\textstyle\prod_i(x_i\,;1) \qquad \text{and} \qquad \prod_i(1\,;y_i)$$

then exist, and

$$(\prod_i x_i) \mathbin{;} 1 = \prod_i (x_i \mathbin{;} 1) \qquad \text{and} \qquad 1 \mathbin{;} (\prod_i y_i) = \prod_i (1 \mathbin{;} y_i), \tag{1}$$

by Lemma 5.30(iii) and its first dual. Consequently,

$$\begin{aligned}(\prod_i x_i) \mathbin{;} 1 \mathbin{;} (\prod_i y_i) &= [(\prod_i x_i) \mathbin{;} 1] \cdot [1 \mathbin{;} (\prod_i y_i)] \\ &= [\prod_i (x_i \mathbin{;} 1)] \cdot [\prod_i (1 \mathbin{;} y_i)] \\ &= \prod_i [(x_i \mathbin{;} 1) \cdot (1 \mathbin{;} y_i)] \\ &= \prod_i (x_i \mathbin{;} 1 \mathbin{;} y_i),\end{aligned}$$

by Lemma 4.26 (for the first and last equalities), (1), and Boolean algebra. □

Corollary 5.56. *If $r = x \mathbin{;} 1 \mathbin{;} y$ and $s = u \mathbin{;} 1 \mathbin{;} v$, then*

$$r \cdot s = (x \cdot u) \mathbin{;} 1 \mathbin{;} (y \cdot v).$$

The complement of a rectangle is in general not a rectangle, but it can always be written as the sum of two (generally non-disjoint) rectangles, and also as the sum of three disjoint rectangles.

Lemma 5.57. *If $r = x \mathbin{;} 1 \mathbin{;} y$, then*

(i) $-r = [(1\text{'} - x) \mathbin{;} 1 \mathbin{;} 1\text{'}] + [1\text{'} \mathbin{;} 1 \mathbin{;} (1\text{'} - y)]$,
(ii) $-r = [(1\text{'} - x) \mathbin{;} 1 \mathbin{;} y] + [x \mathbin{;} 1 \mathbin{;} (1\text{'} - y)] + [(1\text{'} - x) \mathbin{;} 1 \mathbin{;} (1\text{'} - y)]$,

and each of the three rectangles in (ii) *is disjoint from the other two.*

Proof. The elements $x \mathbin{;} 1$ and $1 \mathbin{;} y$ are right- and left-ideal elements respectively, by Lemma 5.28(iii) and its first dual, so

$$-(x \mathbin{;} 1) = (1\text{'} - x) \mathbin{;} 1 \qquad \text{and} \qquad -(1 \mathbin{;} y) = 1 \mathbin{;} (1\text{'} - y),$$

by Lemma 5.30(iv) and its first dual. Use Lemma 4.26, Boolean algebra, the preceding equations, and the identity law for relative multiplication to obtain

$$\begin{aligned}-(x \mathbin{;} 1 \mathbin{;} y) &= -[(x \mathbin{;} 1) \cdot (1 \mathbin{;} y)] = -(x \mathbin{;} 1) + -(1 \mathbin{;} y) \\ &= (1\text{'} - x) \mathbin{;} 1 + 1 \mathbin{;} (1\text{'} - y) = (1\text{'} - x) \mathbin{;} 1 \mathbin{;} 1\text{'} + 1\text{'} \mathbin{;} 1 \mathbin{;} (1\text{'} - y).\end{aligned}$$

This proves (i).

For the proof of (ii), we have

$$\begin{aligned}[(1\text{'} - x) \mathbin{;} 1 \mathbin{;} y] + [(1\text{'} - x) \mathbin{;} 1 \mathbin{;} (1\text{'} - y)] &= (1\text{'} - x) \mathbin{;} 1 \mathbin{;} [y + (1\text{'} - y)] \\ &= (1\text{'} - x) \mathbin{;} 1 \mathbin{;} 1\text{'}\end{aligned}$$

and

$$[x ; 1 ; (1\text{'} - y)] + [(1\text{'} - x) ; 1 ; (1\text{'} - y)] = [x + (1\text{'} - x)] ; 1 ; (1\text{'} - y)$$
$$= 1\text{'} ; 1 ; (1\text{'} - y),$$

by the distributive law for relative multiplication and Boolean algebra. These equations and (i) imply the equation in (ii). The rectangles

$$(1\text{'} - x) ; 1 ; y \qquad \text{and} \qquad (1\text{'} - x) ; 1 ; (1\text{'} - y)$$

are disjoint, because

$$[(1\text{'} - x) ; 1 ; y] \cdot [(1\text{'} - x) ; 1 ; (1\text{'} - y)] = (1\text{'} - x) ; 1 ; [y \cdot (1\text{'} - y)]$$
$$= (1\text{'} - x) ; 1 ; 0 = 0,$$

by Corollary 5.56, Boolean algebra, and Corollary 4.17. Analogous arguments lead to the conclusion that all of the rectangles on the right side of the equation in (ii) are mutually disjoint. □

The converse of a rectangle is easily seen to be a rectangle.

Lemma 5.58. *If* $r = x ; 1 ; y$, *then* $r^{\smile} = y ; 1 ; x$.

Proof. Under the hypothesis of the lemma, we have

$$r^{\smile} = (x ; 1 ; y)^{\smile} = y^{\smile} ; 1^{\smile} ; x^{\smile} = y ; 1 ; x,$$

by the second involution law, and Lemmas 4.1(vi) and 5.20(i). □

The next few lemmas and corollaries give laws governing relative products in which at least one of the factors is a rectangle. The first law implies that the relative product of a rectangle with an arbitrary element s is a rectangle.

Lemma 5.59. *If* $r = x ; 1 ; y$, *then*

$$r ; s = x ; 1 ; z \qquad \textit{and} \qquad s ; r = w ; 1 ; y,$$

where $z = \text{range } y ; s$ *and* $w = \text{domain } s ; x$.

Proof. The first dual of Corollary 5.27(iii) (with $y ; s$ in place of r) and the definition of the range of an element imply that

$$1 ; y ; s = 1 ; z,$$

and consequently

$$r\,;s = x\,;1\,;y\,;s = x\,;1\,;z.$$

This establishes the first equation. The second equation follows by the first duality principle. □

The preceding law can be sharpened in the case when the sides x and y of the rectangle and the given element s are all atoms.

Corollary 5.60. *If the sides of a rectangle* $r = x\,;1\,;y$ *are atoms, and if* s *is an atom, then*

$$r\,;s = \begin{cases} x\,;1\,;z & \text{\textit{when} } y = \text{domain } s, \\ 0 & \text{\textit{when} } y \neq \text{domain } s, \end{cases}$$

where $z = \text{range } s$, *and*

$$s\,;r = \begin{cases} w\,;1\,;y & \text{\textit{when} } x = \text{range } s, \\ 0 & \text{\textit{when} } x \neq \text{range } s, \end{cases}$$

where $w = \text{domain } s$.

Proof. From Lemma 5.59 we have

$$r\,;s = x\,;1\,;z, \tag{1}$$

where $z = \text{range } y\,;s$. According to Lemma 5.50(i) (with y and s in place of x and r respectively),

$$y\,;s = \begin{cases} s & \text{if} \quad y = \text{domain } s, \\ 0 & \text{if} \quad y \neq \text{domain } s. \end{cases}$$

Consequently, if $y = \text{domain } s$, then

$$z = \text{range } y\,;s = \text{range } s,$$

and if $y \neq \text{domain } s$, then $z = 0$. Together with (1) and Corollary 4.17, this observation yields the first assertion of the corollary. The second assertion follows by the first duality principle. □

The next lemma specifies the value of the relative product of two rectangles, one with sides x and y, and the other with sides u and v. It says that the relative product is that portion of the rectangle with sides x and v that lies below the ideal element generated by the product of the sides y and u.

Lemma 5.61. *If* $r = x \,;1\,; y$ *and* $s = u\,;1\,;v$, *then*

$$r\,;s = (x\,;1\,;v)\cdot[1\,;(y\cdot u)\,;1].$$

In particular, $r\,;s = 0$ *whenever* y *and* u *are disjoint.*

Proof. For the proof, we have

$$\begin{aligned} r\,;s = (x\,;1\,;y)\,;(u\,;1\,;v) &= x\,;[1\,;(y\,;u)\,;1]\,;v \\ &= (x\,;1\,;v)\cdot[1\,;(y\,;u)\,;1], \end{aligned} \tag{1}$$

by the hypotheses of the lemma, the associative law for relative multiplication, and Lemma 5.54 (with $1\,;;(y\,;u)\,;1$ in place of s). Since $y\,;u = y\cdot u$, by Lemma 5.20(i) and the assumption that y and u are subidentity elements, the desired conclusion follows from (1). □

The conclusions of the preceding lemma can be sharpened when the relation algebra is simple. This sharpened form follows immediately from the lemma and the fact (to be proved in Theorem 9.2) that the ideal element generated by a non-zero element in a simple relation algebra is always the unit.

Corollary 5.62. *If* $r = x\,;1\,;y$ *and* $s = u\,;1\,;v$ *in a simple relation algebra*, *then*

$$r\,;s = \begin{cases} x\,;1\,;v & \text{if} \quad y\cdot u \neq 0, \\ 0 & \text{if} \quad y\cdot u = 0. \end{cases}$$

So far, the question of the uniqueness of the sides of a non-zero rectangle r has not been addressed. In general, r may be written in the form $r = x\,;1\,;y$ for a variety of sides x and y. Such different representations of r, however, depend essentially on the fact that the relation algebra is not simple. When the relation algebra is simple, the sides of r are uniquely determined.

Lemma 5.63. *Let* $r = x\,;1\,;y$ *and* $s = u\,;1\,;v$ *be rectangles with non-zero sides in a simple relation algebra.*

(i) $r \neq 0$.
(ii) $r \leq s$ *if and only if* $x \leq u$ *and* $y \leq v$.
(iii) $r = s$ *if and only if* $x = u$ *and* $y = v$.

Proof. Two properties of simple algebras are needed to prove the lemma. First, $0 \neq 1$, and second, the ideal element generated by a non-zero element is always the unit (see Theorem 9.2). Observe that

$$1 ; r ; 1 = 1 ; x ; 1 ; y ; 1 = 1 ; x ; 1 ; 1 ; y ; 1 = 1 ; 1 = 1,$$

by the hypotheses on r, Lemma 4.5(iv), and the second property of simple relation algebras. Consequently, r cannot be 0, by Corollary 4.17 and its first dual, and the first property of simple relation algebras. This proves (i).

For the proof of (ii), observe that if $x \le u$ and $y \le v$, then $r \le s$, by the monotony law for relative multiplication. To establish the reverse implication, observe that

$$r ; 1 = x ; 1 ; y ; 1 = x ; 1 \qquad \text{and} \qquad s ; 1 = u ; 1 ; v ; 1 = u ; 1, \tag{1}$$

by the hypotheses on r and s, and the second property of simple relation algebras. If $r \le s$, then $r ; 1 \le s ; 1$, by the monotony law for relative multiplication, and consequently $x ; 1 \le u ; 1$, by (1). Apply Lemma 5.29(i) to conclude that $x \le u$. A dual argument shows that $y \le v$.

Part (iii) is an immediate consequence of (ii). □

A square is a rectangle in which the sides are equal. More precisely, an element r is a *square* if $r = x ; 1 ; x$ for some subidentity element x. All of the lemmas about rectangles apply in particular to squares. Here are some characterizations of squares.

Lemma 5.64. *The following conditions on an element r are equivalent.*

(i) *r is a square.*
(ii) *r is a symmetric rectangle.*
(iii) *r is an equivalence element and a rectangle.*
(iv) $r = r ; 1 ; r^{\smile}$.
(v) $r = s ; 1 ; s^{\smile}$ *for some s.*
(vi) $r = (r \cdot 1\text{'}) ; 1 ; (r \cdot 1\text{'})$.

Proof. We establish the following implications: from (vi) to (i), from (i) to (v), from (v) to (ii), from (ii) to (iv), from (iv) to (iii), and from (iii) to (vi). The implication from (vi) to (i) is a trivial consequence of the definition of a square, and the implication from (i) to (v) is also clear, since the converse of a subidentity element x is just x, by Lemma 5.20(i). If r satisfies (v), then r is a rectangle, by Lemma 5.53(v), and r is symmetric, because

$$r^{\smile} = (s ; 1 ; s^{\smile})^{\smile} = s^{\smile\smile} ; 1^{\smile} ; s^{\smile} = s ; 1 ; s^{\smile} = r, \tag{1}$$

by the assumption on r, the two involution laws, and Lemma 4.1(vi). Consequently, r satisfies (ii).

If r satisfies (ii), then

$$r = r ; 1 ; r = r ; 1 ; r^{\smile} ,$$

by Lemmas 5.53(iii) and 5.1(ii), so r satisfies (iv). If r satisfies (iv), then r is symmetric, by (1) (with r in place of s); and r is a rectangle, by Lemma 5.53(v); and r is transitive, because

$$r ; r = (r ; 1 ; r^{\smile}) ; (r ; 1 ; r^{\smile}) = r ; (1 ; r^{\smile} ; r ; 1) ; r^{\smile} \leq r ; 1 ; r^{\smile} = r,$$

by the assumption on r and the associative and monotony laws for relative multiplication. Consequently, r satisfies (iii).

Finally, if r satisfies (iii), then

$$\begin{aligned} r = r ; 1 ; r &= (r ; 1) \cdot (1 ; r) \\ &= [(r \cdot 1') ; 1] \cdot [1 ; (r \cdot 1')] = (r \cdot 1') ; 1 ; (r \cdot 1'), \end{aligned}$$

by Lemma 5.53(iii), Lemma 4.26 (for the second and last equalities) and Lemma 5.18(iv) and its first dual, so r satisfies (vi). □

The equivalence of (i) and (v) in the preceding lemma implies that there is a polynomial whose range is the set of squares in a relation algebra $\mathfrak{A}$, namely the function ψ defined on $\mathfrak{A}$ by

$$\psi(s) = s ; 1 ; s^{\smile}$$

for each element s.

5.8 Functions

An element r in a relation algebra is said to be a *functional element*, or a *function* for short, if $r^{\smile} ; r \leq 1'$. In set relation algebras, functional elements are just functions in the standard sense of the word (see Section 1.4). There are several useful characterizations of functional elements.

Lemma 5.65. *The following conditions on an element r are equivalent.*

(i) *r is a function.*

(ii) $r \cdot (r \mathbin{;} 0') = 0$.
(iii) $r = r \cdot (-r \mathbin{\underset{,}{+}} 1')$.
(iv) $r = s \cdot (-s \mathbin{\underset{,}{+}} 1')$ *for some element* s.
(v) $r \mathbin{;} 0' \mathbin{\underset{,}{+}} 0 = 0$.
(vi) $(-r \mathbin{\underset{,}{+}} 1') \mathbin{;} 1 = 1$.

Proof. We prove that (i) and (ii) are equivalent, as are (ii) and (iii), and (iii) and (iv), and (v) and (vi). The argument is then completed by showing that (v) implies (ii), and (iii) implies (vi).

The equivalence of (i) and (ii) is a consequence of Boolean algebra and the De Morgan-Tarski laws:

$$\begin{aligned} r^{\smile} \mathbin{;} r \le 1' \qquad &\text{if and only if} \qquad (r^{\smile} \mathbin{;} r) \cdot 0' = 0, \\ &\text{if and only if} \qquad (r \mathbin{;} 0') \cdot r = 0. \end{aligned}$$

The equivalence of (ii) and (iii) follows by Boolean algebra and the definition of relative addition:

$$\begin{aligned} r \cdot (r \mathbin{;} 0') = 0 \qquad &\text{if and only if} \qquad r \le -(r \mathbin{;} 0'), \\ &\text{if and only if} \qquad r \le -r \mathbin{\underset{,}{+}} 1', \\ &\text{if and only if} \qquad r = r \cdot (-r \mathbin{\underset{,}{+}} 1'). \end{aligned}$$

The implication from (iii) to (iv) is trivial. For the implication in reverse direction, assume that r satisfies the equation in (iv) for some element s. Form the complement of both sides of this equation, and use Boolean algebra and the definitions of relative addition and diversity to obtain

$$-r = -[s \cdot (-s \mathbin{\underset{,}{+}} 1')] = -s + -(-s \mathbin{\underset{,}{+}} -0') = -s + (s \mathbin{;} 0'). \tag{1}$$

Form the relative sum of the first and last terms in (1) with 1' on the right to get

$$-r \mathbin{\underset{,}{+}} 1' = [-s + (s \mathbin{;} 0')] \mathbin{\underset{,}{+}} 1'. \tag{2}$$

Form the product on both sides of (2) with r, and use the assumption on r in (iv), to arrive at

$$r \cdot (-r \mathbin{\underset{,}{+}} 1') = [s \cdot (-s \mathbin{\underset{,}{+}} 1')] \cdot ([-s + (s \mathbin{;} 0')] \mathbin{\underset{,}{+}} 1'). \tag{3}$$

The element $-s$ is below $-s + (s \mathbin{;} 0')$, by Boolean algebra, so

$$-s \mathbin{\underset{,}{+}} 1' \le [-s + (s \mathbin{;} 0')] \mathbin{\underset{,}{+}} 1', \tag{4}$$

by the monotony law for relative addition. Combine (3) and (4), and use Boolean algebra and the assumption on r in (iv) to conclude that

$$r \cdot (-r \mathbin{\underset{,}{+}} 1') = s \cdot (-s \mathbin{\underset{,}{+}} 1') = r.$$

To establish the implication from (v) to (ii), assume that r satisfies the equation in (v). We then have

$$0 = (r \,;\, 0') \mathbin{\underset{,}{+}} 0 = (r \,;\, 0') \mathbin{\underset{,}{+}} (1' \cdot 0') = [(r \,;\, 0') \mathbin{\underset{,}{+}} 1'] \cdot [(r \,;\, 0') \mathbin{\underset{,}{+}} 0'], \tag{5}$$

by the hypothesis on r, Boolean algebra, the definition of $0'$, and the distributive law for relative addition over multiplication. Now

$$r \le (r \,;\, 0') \mathbin{\underset{,}{+}} 1' \qquad \text{and} \qquad r \,;\, 0' = (r \,;\, 0') \mathbin{\underset{,}{+}} 0', \tag{6}$$

by the second inequality in Corollary 4.30 (with $0'$ in place of s), the definition of $0'$, and the second dual of Lemma 4.3 for the first formula, and the identity law for relative addition for the second. Compare the right sides of the two formulas in (6) with the factors on the right side of (5), and use Boolean algebra, to conclude that $r \cdot (r \,;\, 0') = 0$, as desired.

The next step is to prove that (iii) implies (vi). If (iii) holds, then r is below $-r \mathbin{\underset{,}{+}} 1'$, by Boolean algebra, and therefore

$$r \,;\, 1 \le (-r \mathbin{\underset{,}{+}} 1') \,;\, 1, \tag{8}$$

by the monotony law for relative multiplication. This law also implies that $r \,;\, 0'$ is below $r \,;\, 1$, so

$$-(r \,;\, 1) \le -(r \,;\, 0') = -r \mathbin{\underset{,}{+}} 1' \le (-r \mathbin{\underset{,}{+}} 1') \,;\, 1, \tag{9}$$

by Boolean algebra, the definition of $0'$ and relative addition, and Lemma 4.5(iii). Combine (8) and (9), and use Boolean algebra, to arrive at the conclusion

$$1 = r \,;\, 1 + -(r \,;\, 1) \le (-r \mathbin{\underset{,}{+}} 1') \,;\, 1.$$

The reverse inequality holds by Boolean algebra, so r satisfies the equation in (vi).

Finally, the equation in (vi) may be obtained from the equation in (v), and vice versa, by forming the complement of both sides of the given equation, and using Boolean algebra and the definition of relative addition. Consequently, the two equations are equivalent. $\square$

The equivalence of (i) and (iv) in the preceding lemma implies that the set of functional elements in a relation algebra $\mathfrak{A}$ is the range of a polynomial, namely the function ψ defined on $\mathfrak{A}$ by

$$\psi(s) = s \cdot (-s \mathbin{+\!\!\!,} 1').$$

The element $s \cdot (-s \mathbin{+\!\!\!,} 1')$ is usually referred to as the *functional part* of s. To understand this terminology, consider an arbitrary relation S in a set relation algebra with base set U, and write

$$R = S \cap ({\sim}S \dagger id_U).$$

The relation R consists of those pairs (α, β) in S such that the presence of a pair of the form (α, γ) in S implies $\gamma = \beta$, by the definitions of R and of relational addition. In other words, R consists of those pairs in S such that the left-hand coordinate of the pair corresponds in S to a unique right-hand coordinate.

The meanings of the characterizations in Lemma 5.65 become more transparent from the perspective of these observations. For example, the equation in (iii) asserts that r is equal to its functional part, while the equation in (iv) asserts that r is equal to the functional part of some element s.

We now turn to the closure properties of the set of functions, and we begin with the closure of this set under various Boolean operations.

Lemma 5.66. (i) 0 *and* $1'$ *are functions.*
(ii) *If* r *is a function and* $s \leq r$, *then* s *is a function and* $(s\,;1) \cdot r = s$.

Proof. The element 0 is a function, by Corollary 4.17, and the element $1'$ is a function, by Lemma 4.3 and the identity law for relative multiplication. This proves (i).

To prove (ii), assume that r is a function and $s \leq r$. Observe that $s^{\smile} \leq r^{\smile}$, and therefore

$$s^{\smile} \,; s \leq r^{\smile} \,; r \leq 1',$$

by the monotony laws for converse and relative multiplication, and the assumption that r is a function. Consequently, s is a function. Also,

$$(s\,; 1) \cdot r \leq s\,; [1 \cdot (s^{\smile}\,; r)] = s\,; s^{\smile}\,; r \leq s\,; r^{\smile}\,; r \leq s\,; 1' = s,$$

by Lemma 4.19 (with s, 1, and r in place of r, s, and t respectively), Boolean algebra, the monotony laws for converse and relative multiplication, the assumption that r is a function, and the identity law for

relative multiplication. The reverse inequality $s \leq (s;1)\cdot r$ follows from Lemma 4.5(iii) and the assumption that s is below r. □

The second part of (ii) in the preceding lemma asserts that s may be obtained by restricting r to the domain of s, or more precisely, to the rectangle whose sides are the domain of s and 1'.

Corollary 5.67. *Every subidentity element is a function.*

It follows from the preceding lemma that if the product of a set of functions exists, then that product is a function. In fact more is true.

Corollary 5.68. *If a set of elements contains at least one function, then the product of the set—if it exists—is a function. In particular, if r is a function, then $r \cdot s$ is a function for every element s.*

To address the question of when the sum of a set of functions is a function, we begin with a preliminary lemma.

Lemma 5.69. *The following conditions on functions r and s are equivalent.*

(i) $r \cdot (s\,;1) = s \cdot (r\,;1)$.
(ii) $r^{\smile}\,;s \leq 1'$ *and* $s^{\smile}\,;r \leq 1'$.

Proof. Assume first that condition (i) holds. Since $r \cdot (s\,;1)$ is below s, by assumption, we have $r \leq -(s\,;1) + s$, by Boolean algebra. Form the converse of both sides of this inequality, and use the monotony law for converse, the distributive law for converse, Lemma 4.1(v),(vi), and the second involution law to obtain

$$\begin{aligned} r^{\smile} &\leq [-(s\,;1)+s]^{\smile} = [-(s\,;1)]^{\smile} + s^{\smile} \\ &= -[(s\,;1)^{\smile}] + s^{\smile} = -(1^{\smile}\,;s^{\smile}) + s^{\smile} = -(1\,;s^{\smile}) + s^{\smile}. \end{aligned} \tag{1}$$

Form the relative product of the first and last terms in (1) with s on the right, and use the monotony and distributive laws for relative multiplication, to arrive at

$$r^{\smile}\,;s \leq [-(1\,;s^{\smile}) + s^{\smile}]\,;s = [-(1\,;s^{\smile})]\,;s + s^{\smile}\,;s. \tag{2}$$

The term $s^{\smile}\,;s$ on the right side of this equation is below 1', by assumption, and the term $[-(1\,;s^{\smile})]\,;s$ is 0, by the first dual of (R10) (with $s^{\smile}$ and 1 in place of r and s respectively) and the first involution law. Combine these observations with (2) to conclude that $r^{\smile}\,;s \leq 1'$.

Interchange r and s in this argument to arrive at $s^{\smile} ; r \leq 1$'. Thus, condition (ii) holds.

Suppose now that condition (ii) holds. In this case,

$$(r^{\smile} ; s) \cdot 0\text{'} = 0 \qquad \text{and} \qquad (s^{\smile} ; r) \cdot 0\text{'} = 0,$$

by Boolean algebra. Apply the De Morgan-Tarski laws to obtain

$$(r ; 0\text{'}) \cdot s = 0 \qquad \text{and} \qquad (s ; 0\text{'}) \cdot r = 0. \tag{3}$$

Now

$$s ; 1 = s ; (0\text{'} + 1\text{'}) = s ; 0\text{'} + s ; 1\text{'} = s ; 0\text{'} + s, \tag{4}$$

by the definition of 0' and Boolean algebra, and the distributive and identity laws for relative multiplication. Consequently,

$$r \cdot (s ; 1) = r \cdot (s ; 0\text{'} + s) = r \cdot (s ; 0\text{'}) + r \cdot s = 0 + r \cdot s = r \cdot s, \tag{5}$$

by (4), Boolean algebra, and the second equation in (3). Interchange r and s in this argument, and use the first equation in (3), to arrive at $s \cdot (r ; 1) = r \cdot s$. Combine this last equation with (5) to obtain (i). □

In the context of set relation algebras, the equation in part (i) of the preceding lemma expresses the condition that two functions agree on their common domain. In the same context, the next lemma says that the union of a set of functions is a function if and only if any two functions in the set agree on their common domain.

Lemma 5.70. *If X is a set of functions for which the sum $\sum X$ exists, then $\sum X$ is a function if and only if $r \cdot (s ; 1) = s \cdot (r ; 1)$ for all distinct elements r and s in X.*

Proof. Assume the sum $\sum X$ exists. Apply the complete distributivity laws for converse and relative multiplication (see Lemma 4.2 and Corollary 4.18) to obtain

$$(\textstyle\sum X)^{\smile} ; \sum X = \sum\{r^{\smile} ; s : r, s \in X\}. \tag{1}$$

The sum $\sum X$ is a function just in case the sum on the right side of (1) is below 1', by the definition of a function. Each element on the right side of (1) that is of the form $r^{\smile} ; r$ is below 1', by assumption, so the entire sum is below 1' just in case $r^{\smile} ; s$ is below 1' for all distinct elements r and s in X. This last condition is equivalent to the validity of the equation $r \cdot (s ; 1) = s \cdot (r ; 1)$ for all distinct elements r and s in X, by Lemma 5.69. □

Corollary 5.71. *If the sum of a directed set of functions exists, then that sum is a function.*

Proof. Let X be a directed set of functions in a relation algebra, and suppose that r and s are distinct elements in X. There exists an element t in X such that $r \leq t$ and $s \leq t$, by the definition of a directed set. Use Boolean algebra and Lemma 5.66(ii) (with r and t in place of s and r respectively) to obtain

$$(r \mathbin{;} 1) \cdot s = (r \mathbin{;} 1) \cdot (t \cdot s) = [(r \mathbin{;} 1) \cdot t] \cdot s = r \cdot s.$$

A similar argument shows that $(s \mathbin{;} 1) \cdot r = r \cdot s$, so

$$r \cdot (s \mathbin{;} 1) = s \cdot (r \mathbin{;} 1).$$

Apply Lemma 5.70 to conclude that if the sum $\sum X$ exists, then this sum is a function. □

A somewhat deeper consequence of Lemma 5.70 is that the sum of a set of functions with disjoint domains is again a function.

Lemma 5.72. *If the sum of a set of functions with disjoint domains exists, then that sum is a function. In particular, if r and s are functions, and if*

$$(r \mathbin{;} 1) \cdot (s \mathbin{;} 1) = 0,$$

then $r + s$ is a function.

Proof. Suppose X is a set of functions with disjoint domains. This assumption implies that for any two distinct elements r and s in X, we have

$$(r \mathbin{;} 1) \cdot (s \mathbin{;} 1) \cdot 1' = 0,$$

by the definition of the domains of r and s, and Boolean algebra. Apply the De Morgan-Tarski laws to this equation (with 1 and $(s \mathbin{;} 1) \cdot 1'$ in place of s and t) to obtain

$$([(s \mathbin{;} 1) \cdot 1'] \mathbin{;} 1^{\smile}) \cdot r = 0.$$

In view of Lemma 4.1(vi) and Corollary 5.27(iii), the preceding equation reduces to the equation $r \cdot (s \mathbin{;} 1) = 0$. An analogous argument yields the equation $s \cdot (r \mathbin{;} 1) = 0$. It follows that

$$r \cdot (s \mathbin{;} 1) = s \cdot (r \mathbin{;} 1),$$

so Lemma 5.70 may be applied to conclude that the sum $\sum X$ is a function whenever this sum exists.

The domains of r and of s are below $r\,;1$ and $s\,;1$ respectively, by Boolean algebra. Consequently, if the right-ideal elements $r\,;1$ and $s\,;1$ are disjoint, then so are the domains of r and s, and therefore $r+s$ is a function, by the first part of the lemma. □

We turn now to questions regarding the closure of the set of functions under Peircean operations. The following functional terminology will be useful: *r maps x to y* means that r is a function with domain x and range y. The first lemma is just an abstract version of the ubiquitous set-theoretical observation that the composition of two (set-theoretical) functions is a function.

Lemma 5.73. (i) *If r and s are functions, then $r\,;s$ is a function.*
(ii) *If r maps x to y, and s maps y to z, then $r\,;s$ maps x to z.*

Proof. Suppose r and s are functions. Use the second involution law, the associative, identity, and monotony laws for relative multiplication, and the assumptions on r and s to obtain

$$\begin{aligned}(r\,;s)^{\smile}\,;(r\,;s) = (s^{\smile}\,;r;^{\smile})\,;(r\,;s) = s^{\smile}\,;(r^{\smile}\,;r)\,;s \\ \leq s^{\smile}\,;1\text{'}\,;s = s^{\smile}\,;s \leq 1\text{'},\end{aligned}$$

This proves that $r\,;s$ is a function.

The proof of (ii) requires a bit more work. Suppose x and y are the domain and range of r, and y and z the domain and range of s. This means that

$$x = (r\,;1)\cdot 1\text{'}, \quad y = (1\,;r)\cdot 1\text{'}, \quad y = (s\,;1)\cdot 1\text{'}, \quad z = (1\,;s)\cdot 1\text{'}. \quad (1)$$

Use Lemma 5.48(ii), the second and third equations in (1), and the monotony law for relative multiplication to obtain

$$r = r\,;y = r\,;[(s\,;1)\cdot 1\text{'}] \leq r\,;s\,;1. \quad (2)$$

From (2), the monotony law for relative multiplication, and part (iv) of Lemma 4.5, we get

$$r\,;1 \leq r\,;s\,;1\,;1 = r\,;s\,;1.$$

The reverse inequality $r\,;s\,;1 \leq r\,;1$ is a consequence of the monotony law for relative multiplication, so

$$r ; 1 = r ; s ; 1. \tag{3}$$

Use the first equation in (1), the equation in (3), Boolean algebra, and the definition of the domain of $r ; s$ to conclude that

$$x = (r ; 1) \cdot 1' = (r ; s ; 1) \cdot 1' = \text{domain } r ; s.$$

A dual argument yields

$$z = (1 ; s) \cdot 1' = (1 ; r ; s) \cdot 1' = \text{range } r ; s,$$

which completes the proof. □

Surprisingly, the relative sum of two functions is also a function.

Lemma 5.74. *If r and s are functions, then $r \mathbin{+\!\!,} s$ is a function.*

Proof. Assume r and s are functions, and write $t = r \mathbin{+\!\!,} s$. The immediate goal is to show that

$$t^{\smile} ; (t - r) \leq 1'. \tag{1}$$

We begin with three preliminary computations. Since

$$1' = s \cdot 1' + -s \cdot 1',$$

by Boolean algebra, the identity and distributive laws for relative multiplication imply that

$$\begin{aligned} -r = -r ; 1' = -r ; (s \cdot 1' + -s \cdot 1') \\ = -r ; (s \cdot 1') + -r ; (-s \cdot 1'). \end{aligned} \tag{2}$$

The two summands on the right side of (2) are respectively below

$$1 ; (s \cdot 1') \qquad \text{and} \qquad -r ; -s,$$

by the monotony law for relative multiplication; and $-r ; -s$ is equal to $-t$, by the definitions of t and of relative addition; so (2) implies that

$$-r \leq 1 ; (s \cdot 1') + -t.$$

Form the product of each side of this inequality with t on the left, and use Boolean algebra to obtain

$$t - r \le t \cdot [1 ; (s \cdot 1') + -t] = t \cdot [1 ; (s \cdot 1')] + t \cdot -t \le 1 ; (s \cdot 1'). \quad (3)$$

For the second preliminary computation, use the definition of t, the second dual of the second involution law (see Lemma 4.7(iii)), and Corollary 4.30 (with $s^{\smile}$ and r in place of r and s respectively) to obtain

$$t^{\smile} ; -r = (r \,\dagger\, s)^{\smile} ; -r = (s^{\smile} \,\dagger\, r^{\smile}) ; -r \le s^{\smile}. \quad (4)$$

For the third preliminary computation, use Corollary 4.20 (with r, s, and t replaced by 1, $s \cdot 1'$, and $s^{\smile}$ respectively), Boolean algebra, Lemma 5.20(i), the monotony law for relative multiplication, and the assumption that s is a function to get

$$\begin{aligned}[1 ; (s \cdot 1')] \cdot s^{\smile} &\le ([s^{\smile} ; (s \cdot 1')^{\smile}] \cdot 1) ; (s \cdot 1') \quad (5)\\ &= s^{\smile} ; (s \cdot 1')^{\smile} ; (s \cdot 1') = s^{\smile} ; (s \cdot 1') \le s^{\smile} ; s \le 1'.\end{aligned}$$

Turn now to the proof of (1). We have

$$t^{\smile} ; (t - r) \le 1 ; (t - r) \le 1 ; [1 ; (s \cdot 1')] = 1 ; (s \cdot 1'),$$

by the monotony law for relative multiplication (applied twice), (3), and Lemma 4.5(iv). We also have

$$t^{\smile} ; (t - r) \le t^{\smile} ; -r \le s^{\smile},$$

by the monotony law for relative multiplication and (4). Combine these two computations, and use Boolean algebra and (5) to arrive at

$$t^{\smile} ; (t - r) \le [1 ; (s \cdot 1')] \cdot s^{\smile} \le 1'.$$

This proves (1).

Form the converse of both sides of (1), and use the monotony laws for converse and relative multiplication, the involution laws, Lemma 4.1(iii), and Lemma 4.3, to obtain

$$(t^{\smile} - r^{\smile}) ; t \le 1'. \quad (6)$$

To prove the lemma, it must be shown that $t^{\smile} ; t \le 1'$. Since

$$t = t \cdot r + (t - r),$$

by Boolean algebra, we may form the relative product of both sides of this equation with $t^{\smile} ; r^{\smile}$ on the left, and use the distributive law for relative multiplication, to write

$$(t^{\smile} \cdot r^{\smile}) ; t = (t^{\smile} \cdot r^{\smile}) ; (t \cdot r) + (t^{\smile} \cdot r^{\smile}) ; (t - r). \tag{7}$$

The first summand on the right side of (7) is below $r^{\smile} ; r$, which in its turn is below 1', by the monotony law for relative multiplication and the assumption that r is a function. The second summand on the right side of (7) is below $t^{\smile} ; (t - r)$, which in its turn is below 1', by the monotony law for relative multiplication and (1). It follows that

$$(t^{\smile} \cdot r^{\smile}) ; t \leq 1'. \tag{8}$$

Since

$$t^{\smile} = t^{\smile} \cdot r^{\smile} + (t^{\smile} - r^{\smile}),$$

by Boolean algebra, we may form the relative product of both sides of this equation with t on the right, and use the distributive laws for relative multiplication, to write

$$t^{\smile} ; t = (t^{\smile} \cdot r^{\smile}) ; t + (t^{\smile} - r^{\smile}) ; t.$$

Each of the summands on the right side of this equation is below 1', by (8) and (6) respectively, so $t^{\smile} ; t \leq 1'$, as was to be proved. □

Functions satisfy a left-hand distributive law for relative multiplication over multiplication, and in fact functions can be characterized by this law.

Lemma 5.75. *An element r is a function if and only if*

$$r ; (s \cdot t) = (r ; s) \cdot (r ; t)$$

for all elements s and t.

Proof. Suppose first that r is a function, and let s and t be arbitrary elements. Certainly,

$$r ; (s \cdot t) = (r \cdot r) ; (s \cdot t) \leq (r ; s) \cdot (r ; t),$$

by Boolean algebra and Lemma 4.5(ii). To establish the reverse inequality, apply Lemma 4.19 (with $r ; t$ in place of t), the assumption that r is a function, and the monotony and identity laws for relative multiplication to obtain.

$$(r ; s) \cdot (r ; t) \leq r ; [s \cdot (r^{\smile} ; r ; t)] \leq r ; [s \cdot (1' ; t)] = r ; (s \cdot t).$$

The given distributive law therefore holds.

Assume now that the given distributive law holds for all elements s and t. Take s and t to be 1' and 0' respectively, and use also Corollary 4.17, Boolean algebra, and the definition of 0', to obtain

$$0 = r\,;0 = r\,;(1'\cdot 0') = (r\,;1')\cdot(r\,;0') = r\cdot(r\,;0').$$

Apply Lemma 5.65(ii) to conclude that r is a function. □

The first dual of the preceding lemma is quite useful in its own right.

Corollary 5.76. *An element r is the converse of a function if and only if*

$$(t\cdot s)\,;r = (t\,;r)\cdot(s\,;r)$$

for all elements s and t.

Functions are also characterized by another distributive law, namely a distributive law for relative multiplication over difference.

Lemma 5.77. *An element r is a function if and only if*

$$r\,;(s-t) = r\,;s - r\,;t$$

for all elements s and t.

Proof. Assume first that r is a function, and s and t arbitrary elements. The inequality

$$r\,;s - r\,;t \le r\,;(s-t)$$

follows from the semi-distributive law for relative multiplication over subtraction (see Lemma 4.6), so only the reverse inequality needs to be established. Because r is a function, we may use the distributive law in Lemma 5.75, together with Boolean algebra and Corollary 4.17, to obtain

$$[r\,;(s-t)]\cdot(r\,;t) = r\,;[(s-t)\cdot t] = r\,;0 = 0.$$

Consequently, $r\,;(s-t)$ is below $-(r\,;t)$, by Boolean algebra. The monotony law for relative multiplication implies that $r\,;(s-t)$ is also below $r\,;s$, so

$$r\,;(s-t) \le r\,;s - r\,;t,$$

as was to be shown.

Assume now that the given distributive law holds for all elements s and t. Take s and t to be 0' and 1' respectively, and use also Boolean algebra and the identity law for relative multiplication, to get

$$r ; 0' = r ; (0' - 1') = r ; 0' - r ; 1' = r ; 0' - r.$$

This computation shows that $r;0'$ is below $-r$, so $(r;0')\cdot r = 0$. Apply Lemma 5.65(ii) to conclude that r is a function. □

The implication from left to right in Lemma 5.77 was proved with the help of the corresponding implication in Lemma 5.75. It turns out that, conversely, the implication from left to right in Lemma 5.77 also implies the corresponding implication in Lemma 5.75, because

$$s \cdot t = s - (s - t),$$

by Boolean algebra.

There is a special case of the distributive law in Lemma 5.77 that already characterizes functions.

Corollary 5.78. *An element r is a function if and only if*

$$(r ; s) \cdot (r ; -s) = 0$$

for all elements s.

Proof. If r is a function, then

$$(r ; s) \cdot (r ; -s) = r ; (s - s) = r ; 0 = 0,$$

by Lemma 5.77 (with s in place of t), Boolean algebra, and Corollary 4.17. On the other hand, if the given equation holds, then take s to be 0', and argue as in the last part of the proof of Lemma 5.77 to conclude that r is a function. □

With the help of Lemma 4.6, it is possible to establish an infinitary version of the distributive law in Lemma 5.75.

Lemma 5.79. *If r is a function. then for every non-empty set X of elements, the existence of $\prod X$ implies that $\prod\{r ; s : s \in X\}$ exists and*

$$r ; (\textstyle\prod X) = \prod\{r ; s : s \in X\}.$$

Proof. Assume r is a function, and X a non-empty set of elements whose product exists. Write

$$Y = \{-s : s \in X\},$$

and observe that the sum $\sum Y$ exists, becasue it is the complement of $\prod X$. The Boolean identity

$$\prod X = 1 - \sum Y$$

and Lemma 5.77 together yield

$$r\,;(\prod X) = r\,;(1 - \sum Y) = r\,;1 - r\,;(\sum Y). \tag{1}$$

The definition of Y and the complete distributivity of relative multiplication imply that

$$r\,;(\sum Y) = \sum\{r\,;-s : s \in X\},$$

so

$$-[r\,;(\sum Y)] = \prod\{-(r\,;-s) : s \in X\}, \tag{2}$$

by Boolean algebra. Combine (1) and (2), and use Boolean algebra, to arrive at

$$\begin{aligned} r\,;(\prod X) &= (r\,;1)\cdot\prod\{-(r\,;-s) : s \in X\} \\ &= \prod\{(r\,;1)\cdot-(r\,;-s) : s \in X\}. \end{aligned} \tag{3}$$

Use Lemma 5.77 and Boolean algebra to write

$$(r\,;1)\cdot-(r\,;-s) = r\,;1 - (r\,;-s) = r\,;[1-(-s)] = r\,;s \tag{4}$$

for every s in X. Together, (3) and (4) immediately yield the desired conclusion. □

Functions can also be characterized as the elements satisfying a certain modular law. In fact, this law is just a strengthened version of Corollary 4.20 in which the inequality has been replaced by equality (and the variables r and s have been interchanged).

Lemma 5.80. *An element r is a function if and only if*

$$t\cdot(s\,;r) = [(t\,;r^{\smile})\cdot s]\,;r$$

for all elements s and t.

Proof. Assume first that r is a function, and s and t arbitrary elements, with the goal of showing that the given modular law holds. The inequality

$$t \cdot (s\,;r) \leq [(t\,;r^{\smile}) \cdot s]\,;r$$

follows from Corollary 4.20 (with r and s interchanged), so only the reverse inequality needs to be established. We have

$$[(t\,;r^{\smile}) \cdot s]\,;r \leq t\,;r^{\smile}\,;r \leq t\,;1' = t,$$

by the monotony and identity laws for relative multiplication, and the assumption that r is a function. The inequality

$$[(t\,;r^{\smile}) \cdot s]\,;r \leq s\,;r$$

is a consequence of the monotony law for relative multiplication. Combine these inequalities, and use Boolean algebra, to arrive at

$$[(t\,;r^{\smile}) \cdot s]\,;r \leq t \cdot (s\,;r).$$

Thus, the given modular law holds.

Assume now that the given modular law holds for all elements s and t. Take s and t to be 1 and $1'$ respectively, and use Boolean algebra and the identity law for relative multiplication, to obtain

$$1' \cdot (1\,;r) = [(1'\,;r^{\smile}) \cdot 1]\,;r = r^{\smile}\,;r.$$

It follows from these equations that $r^{\smile}\,;r$ is below $1'$, so r is a function. □

The first dual of the preceding lemma demonstrates even more clearly the connection of the lemma with Lemma 4.19.

Corollary 5.81. *An element r is the converse of a function if and only if*

$$(r\,;s) \cdot t = r\,;[(s \cdot (r^{\smile}\,;t)]$$

for all elements s and t.

The second part of the proof of Lemma 5.80 actually shows a bit more than is stated.

Corollary 5.82. *An element r is a function if and only if*

$$\text{range } r = r^{\smile}\,;r.$$

The first dual of this corollary asserts that r is the converse of a function if and only if domain $r = r\,;r^{\smile}$.

Our next goal is to establish a stronger form of the De Morgan-Tarski laws for functions with the same domain. We begin with a preliminary lemma that has other applications.

Lemma 5.83. *If r is a function, then $[(r\cdot s)\,;1]\cdot r \le s$ for every element s.*

Proof. Assume r is a function. We have

$$\begin{aligned}[(r\cdot s)\,;1]\cdot r &\le (r\cdot s)\,;(1\cdot[(r\cdot s)^{\smile}\,;r]) = (r\cdot s)\,;(r\cdot s)^{\smile}\,;r \\ &= (r\cdot s)\,;(r^{\smile}\cdot s^{\smile})\,;r \le s\,;r^{\smile}\,;r \le s\,;1' = s,\end{aligned}$$

by Lemma 4.19 (with $r\cdot s$, 1, and r in place of r, s, and t respectively), Boolean algebra, Lemma 4.1(ii), the monotony law for relative multiplication, the assumption that r is a function, and the identity law for relative multiplication. □

The next lemma says that functions with the same domain behave similarly to atoms in the context of the De Morgan-Tarski laws.

Lemma 5.84. *If r and s are functions with the same domain, then for any element t,*

$$r \le s\,;t \qquad \textit{if and only if} \qquad s \le r\,;t^{\smile}.$$

Proof. Let r and s be functions with the same domain, and t an arbitrary element. If $r \le s\,;t$, then $r = (s\,;t)\cdot r$, by Boolean algebra, and therefore

$$r\,;1 = [(s\,;t)\cdot r]\,;1 = [(r\,;t^{\smile})\cdot s]\,;1, \tag{1}$$

by Lemma 5.26 (with s, t, and r in place of r, s, and t respectively). Now r and s are assumed to have the same domain, so $r\,;1 = s\,;1$, by Lemma 5.47, and therefore

$$s\,;1 = [(r\,;t^{\smile})\cdot s]\,;1, \tag{2}$$

by (1). The function s is below $s\,;1$, by Lemma 4.5(iii), and therefore s is below the right side of (2). It follows by Boolean algebra and Lemma 5.83 (with s and $r\,;t^{\smile}$ in place of r and s respectively) that

$$s = s\cdot([(r\,;t^{\smile})\cdot s]\,;1) \le r\,;t^{\smile}. \tag{3}$$

The argument so far shows that

$$r \le s\,;t \qquad \text{implies} \qquad s \le r\,;t^{\smile}$$

whenever s is a function with the same domain as r. Interchange r and s in this implication, and replace t with $t^{\smile}$ to obtain

$$s \le r\,;t^{\smile} \qquad \text{implies} \qquad r \le s\,;t^{\smile\smile}.$$

Since $t^{\smile\smile} = t$, by the first involution law, the desired conclusion follows directly from the two preceding implications. □

Corollary 5.85. *If r and s are functions with the same domain, then $r \le s$ implies $r = s$.*

Proof. Assume r and s are functions with the same domain. If $r \le s$, then $r \le s\,;1'$, by the identity law for relative multiplication, and therefore

$$s \le r\,;1'^{\smile} = r\,;1' = r,$$

by Lemma 5.84 (with 1' in place of t), Lemma 4.3, and the identity law for relative multiplication. It follows that $r = s$. □

The next lemma deals with atoms that involve functions.

Lemma 5.86. *Let r be a function.*

(i) *r is an atom if and only if* domain r *is an atom.*
(ii) *If s is an atom such that* range s *and* domain r *are not disjoint, then $s\,;r$ is an atom.*
(iii) *If s is an atom in the Boolean algebra of right-ideal elements, and if $r \cdot s \ne 0$, then $r \cdot s$ is an atom.*

Proof. We begin with the proof of (ii). Assume s is an atom whose range is not disjoint from the domain of r. In this case, the relative product $s\,;r$ is not zero, by Lemma 5.51. To check that $s\,;r$ is an atom, it must be shown that for an arbitrary element t,

$$(s\,;r)\cdot t \ne 0 \qquad \text{implies} \qquad s\,;r \le t. \tag{1}$$

If the hypothesis of (1) holds, then

$$(t\,;r^{\smile})\cdot s \ne 0,$$

by the De Morgan-Tarski laws, and therefore

$$s \leq t\,;r^{\smile},$$

by the assumption that s is an atom. Form the relative product of both sides of this last inequality with r on the right, and use the monotony law for relative multiplication, the assumption that r is a function, and the identity law for relative multiplication, to arrive at

$$s\,;r \leq t\,;r^{\smile}\,;r \leq t\,;1\text{'} = t.$$

Thus, (1) holds, so $s\,;r$ is an atom.

Turn next to the proof of (i). If r is an atom, then domain r is an atom, by Lemma 5.48(v). To establish the implication in the opposite direction, write $s =$ domain r, and observe that

$$\text{range } s = (1\,;s) \cdot 1\text{'} = s \cdot 1\text{'} = s = \text{domain } r, \tag{2}$$

by the definition of range s, the first dual of Lemma 5.20(ii) (with s and 1' in place of r and s respectively), Boolean algebra, and the definition of s, which implies that s is a subidentity element. If s is an atom, then $s\,;r$ is an atom, by part (ii) of the lemma. But $s\,;r = r$, by Lemma 5.48(ii) and the definition of s, so r is an atom.

To prove (iii), write $p = r \cdot s$, with the goal of showing that

$$p \cdot t \neq 0 \qquad \text{implies} \qquad p \leq t \tag{3}$$

for every element t. Assume the hypothesis of (3), and observe that

$$(p \cdot t)\,;1 \neq 0, \tag{4}$$

by Lemma 4.5(iii). The element s is a right-ideal element, by assumption, so

$$s \cdot [(p \cdot t)\,;1] = (s \cdot p \cdot t)\,;1 = (p \cdot t)\,;1, \tag{5}$$

by the modular law for right-ideal elements in Lemma 5.35 (with r, s, and t replaced by s, $p \cdot t$, and 1 respectively), the definition of p, and Boolean algebra. Consequently, the first term in (5) is not zero, by (4) and (5). Since s is assumed to be an atom in the Boolean algebra of right-ideal elements, it follows from this observation that s is below the right-ideal element $(p \cdot t)\,;1$, and therefore so is p, by the definition of p. The element p is a function, by Corollary 5.68 and the assumption that r is a function, so

$$p = [(p \cdot t) ; 1] \cdot p \leq t,$$

by Boolean algebra and Lemma 5.83 (with p and t in place of r and s respectively). Thus, the conclusion of (3) holds, as desired, so p is an atom. □

The converse of a function r need not be a function. If the converse of r is a function, then r is called a *bijectional element*, or a *bijection* for short. The terms *bifunctional element*, *injectional element*, and *injection* are also used. In a set relation algebra a bijection is just a one-to-one function. The various lemmas and corollaries in this section have counterparts for bijections. For instance, an element r is a bijection if and only if the two distributive laws

$$r ; (s \cdot t) = (r ; s) \cdot (r ; t) \qquad \text{and} \qquad (t \cdot s) ; r = (t ; r) \cdot (s ; r)$$

for relative multiplication over multiplication hold for all elements s and t. For another example, the converse of a bijection from x to y is a bijection from y to x, and the relative product of a bijection from x to y with a bijection from y to z is a bijection from x to z. It will be convenient to refer to such results as the versions for bijections of lemmas and corollaries that are formulated for functions. For instance, the above mentioned distributive laws are just the versions of Lemma 5.75 and Corollary 5.76 that apply to bijections.

A bijection whose domain and range are both 1' is called a *permutational element*, or a *permutation* for short. As might be expected, the permutations form a group under the Peircean operations.

Lemma 5.87. *The set of permutations in a relation algebra is a group under the operations of relative multiplication and converse*, *with* 1' *as the identity element of the group*.

Proof. Let G be the set of permutations in a relation algebra, and consider elements r and s in G. Both elements are bijections from 1' to 1', by the definition of a permutation, so their relative product $r ; s$ is a bijection from 1' to 1', and hence a permutation, by the version of Lemma 5.73 for bijections. Thus, G is closed under the operation of relative multiplication. Also, $r^{\smile}$ is a bijection from 1' to 1', and in fact

$$1' = \text{domain } r = r ; r^{\smile} \qquad \text{and} \qquad 1' = \text{range } r = r^{\smile} ; r, \tag{1}$$

by the version of Corollary 5.82 for bijections. It follows that G is closed under the operation of converse. The identity element is a permutation,

by Lemma 4.3 and the identity law for relative multiplication, so it belongs to G. The validity of the group axioms (see Section 3.5) in the resulting algebra

$$(G\,,\,;\,,\,{}^{\smile}\,,\,1\text{'})$$

is an immediate consequence of the associative and identity laws for relative multiplication, and (1). □

5.9 Historical remarks

The study of special relations has been an important part of the calculus of relations at least since the time of Schröder. In [98], Schröder introduces and studies transitive elements, right-ideal elements, and functions, and he states many important laws about these special elements. It is very easy, however, for a modern reader to be overwhelmed by his work because of the great number and variety of laws that it contains, and because the problems that motivated Schröder to study these laws are no longer of central interest to researchers in this domain.

The general deductive development of the arithmetic of special elements within the framework of the equational theory of relation algebras was initiated and extensively developed by Tarski, who focused on important laws of general interest, broad appeal, and wide applicability. Many of the results that he obtained in this direction can be found in [23].

Below is a brief survey, to the best of our knowledge, of the historical origins of the notions and results presented in this chapter.

The notion of a symmetric element was introduced by Tarski in his courses on relation algebras, and Lemma 5.1 is due to him, as are the closure properties in Lemma 5.2. The notion of a transitive relation was introduced by De Morgan, although in a more restricted form. The definition we have used goes back to Schröder [98], and the characterizations of transitive elements given in conditions (ii), (iii), (vi), (vii), and (viii) of Lemma 5.5 are stated in [98]. The closure properties for the set of transitive elements that are formulated in Lemma 5.6 date back to Tarski's 1945 seminar on relation algebras, while those in Lemma 5.7 are from his 1970 seminar on relation algebras. The results in Exercises 5.6 and 5.7 are from the 1945 seminar, while the result in Exercise 5.3 is due to Givant.

Most of the results in the section on equivalence elements are due to Tarski or Chin, and are contained in [23]. Equivalence elements were introduced in the 1945 seminar, presumably because Tarski already realized at that time that a relation algebra could be relativized to an arbitrary equivalence element and the result would again be a relation algebra (see Chapter 10). The characterizations of equivalence elements given in conditions (ii)–(iv) and (ix) of Lemma 5.8 are from the 1945 seminar, while conditions (v) and (vi) of the lemma were found by Chin in 1945 and are included in her doctoral dissertation [22]. The equivalence of the first six conditions of the lemma is stated and proved in [23]; the equivalence of (i) with (vii) and (viii) is due to Givant. The characterizations of reflexive equivalence elements given in Exercise 5.9 are from the 1945 seminar.

The closure properties for the set of equivalence elements that are contained in parts (i), (ii), and (v) of Lemma 5.9 and in Lemma 5.11 are from the 1945 seminar and are given in [23]. A weaker form of Lemma 5.9(iii) is also given in [23], namely the assertion that the sum of a chain of equivalence elements, if it exists, is an equivalence element; the generalization to directed sets of equivalence elements was observed by Tarski in the 1970 seminar [112]. Part (iv) of the lemma is a special case of Lemma 5.23 (see below). Lemma 5.12 is given in [23] and is a generalization, due to Tarski, of the earlier result of Julia Robinson given in Lemma 4.34. The generalization of Lemma 5.12 given in Exercise 5.15 is due to Jónsson [51], as are also the results in Exercises 5.16 and 5.17. Corollary 5.10, Lemma 5.18(ii),(iv), Lemma 5.20(i), and Lemma 5.22 are due to Tarski and are given in [23]. The consequence of Lemma 5.22 that is contained in Lemma 5.23 is due to Tarski and is from the 1970 seminar. The characterizations of equivalence elements in terms of the modular law in Lemmas 5.14 and 5.15 are from Chin [22] and are given in [23]. Lemma 5.13 is equivalent to the implication from left to right in Lemma 5.14. The applications of Lemma 5.14 contained in Theorem 5.16 and Corollary 5.17 are from Tarski's 1970 seminar, but the application to complex algebras of groups is already discussed in [22] and [23]. Lemma 5.24 is due to Jónsson [51]. The special case of the lemma when $r = 1'$ (see Corollary 5.25) is given in [105] and is essentially contained in Jónsson-Tarski [55]. A preliminary form of this special case occurs already in Schröder [98] under the name "the abacus of binary relatives". Lemma 5.18(i),(iii), Corollary 5.19, Lemma 5.20(ii),(iii), and Lemma 5.21 are due to Givant [34], while the results in Exercises 5.11–

5.13 are from Tarski's 1945 seminar, and the observation implicit in Exercise 5.8 is from [23]. The description of the non-zero equivalence elements in the complex algebra of a modular lattice L with zero (see Exercise 5.19), and the theorem that L is embeddable into the lattice of non-zero equivalence elements $\mathfrak{Cm}(L)$ (see Exercise 5.20) is due to Maddux [73].

Right-ideal elements are introduced in Schröder [98], where they are called "Systeme", the German word for systems. Schröder is clearly aware that these elements are a way of talking about sets in the context of binary relations. He lists a great number of identities involving right-ideal elements, among them the identity in Lemma 5.26 and the characterizations in parts (ii) and (vi) of Lemma 5.28. He also shows that sums, products, and complements of right-ideal elements are again right-ideal elements, so that any Boolean combination of right-ideal elements is a right-ideal element. The closure of the set of right-ideal elements under infinitary Boolean operations was noted by Tarski in his 1945 seminar and is proved in [23]. The sharper formulations of the closure properties that are given in parts (ii)–(iv) of Lemma 5.30, using subidentity elements, are due to Givant and are closely related to results in [34]. Part (ii) of Corollary 5.27 is from Tarski-Givant [113]; the special case of (ii) that is given in part (iii) is implicit in [23]. Lemma 5.29 is from Givant [34]. Lemma 5.31 is also due to Givant; the proof given in the text follows a suggestion of Hajnal Andréka, while the original proof may be found in the solution to Exercise 5.23. The laws in Lemma 5.32 and Lemma 5.34 are due to Tarski and are given in [23]. The characterizations in Lemmas 5.35 and 5.37 of right-ideal elements as elements satisfying certain modular laws are due to Tarski and to Chin respectively. The first of these dates back to the 1945 seminar, and the second appears in Chin [22]; both characterizations are given in [23].

Ideal elements are implicit in some of the work of Peirce; for example, in [88] he gives a number of laws involving elements of the forms $1\,;r\,;1$ and $0\,;s\,;0$. Schröder, too, formulates a number of laws involving these elements in [98]. In particular, he realizes that a Boolean combination of elements of the form $1 ; r ; 1$ is again an element of this form (see Lemma 5.39), and he states the laws in Corollary 5.42. The characterizations of ideal elements that are given in conditions (ii) and (vi) of Lemma 5.38 and in Exercise 5.34 go back to Tarski's 1945 seminar; the characterization in Exercise 5.34 is attributed to Chin in [23]. The characterizations given in parts (iii), (iv), (v), (vii), and (viii) of Lemma 5.38 and in Corollary 5.43 are due to Givant.

Lemma 5.40 is a joint result of Andréka and Givant. The laws in Lemma 5.41, and the characterization of ideal elements in terms of the distributive law given in Lemma 5.44, are due to Tarski and are from the 1945 seminar, while the characterization of ideal elements in terms of the distributive law given in Lemma 5.45 is due to Chin [22]; these laws are all stated and proved in [23]. Ideal elements were originally called "Boolean elements" by Tarski, presumably because of the properties set forth in Lemma 5.41. The algebraic significance of these elements, that is to say, the relationship of these elements to relation algebraic ideals, was discovered jointly by McKinsey and Tarski in 1941, and presumably this discovery eventually motivated the adoption of the name "ideal elements". The relationship between ideal elements and ideals is mentioned in [23] and is presented more fully in [55].

The definition given in Section 5.6 of the domain and range of an element is due to Givant, and the equivalent definition implicit in Lemma 5.48(i) is due to Maddux [74]. Parts (ii) and (v) of Lemma 5.48 are from [74] as are the equivalence of (b) and (c) in parts (i) and (ii) of Lemma 5.50, and parts (iii) and (vi) of Lemma 5.52. The results in Lemmas 5.47, 5.48(iii),(iv),(vi), 5.49, 5.50(iii), the equivalence of parts (a) and (b) in (i) and (ii) of 5.50, 5.51, and parts (iv), (v), and (vii) of 5.52 are due to Givant. Previously, Tarski and his students used the elements $r ; 1$ and $1 ; r$ to speak about the domain and range of an element r. This approach makes it difficult to formulate some of the laws about domains and ranges in the sharpest possible way.

The notion of a rectangle is introduced in Schröder [98] under the German name "Augenquaderrelativ"; an *Augenquaderrelativ* is defined to be an element of the form $(r \mathbin{+\!\!,} 0) \cdot (0 \mathbin{+\!\!,} s)$, where r and s are arbitrary elements. Schröder points out that each of the forms mentioned in Lemma 5.53(ii)–(iv) is equivalent to his definition. He observes further that right-ideal elements are special cases of Augenquaderrelatives, as are also left-ideal elements. Schröder gives a number of laws involving rectangles, including a law which implies that the product of two rectangles is a rectangle (see Corollary 5.56). The definitions of a rectangle and a square that are given in Section 5.7 (in terms of subidentity elements) are due to Givant [34], as are the characterizations in Lemma 5.53(v),(vi), the proofs of all of the characterizations in lemma in the context of relation algebras, the characterizations in 5.64, the laws in Lemmas 5.54–5.63 and their corollaries, and the law in Exercise 5.37.

The notion of a function and variants of this notion (such as the notion of a function that is everywhere defined, or one-to-one, or onto, or some combination of these three) are introduced and studied within the framework of the calculus of relations by Schröder [98]. In particular, Schröder also discusses the notion of a permutation. The various characterizations of functions given in Lemma 5.65 occur already in [98], as do a variety of statements of the following form: the relative product of functions is a function (see Lemma 5.73(i)); the relative product of everywhere defined functions is an everywhere defined function; the relative product of permutations is a permutation; and so on. The notion of the functional part of an arbitrary relation (see the remarks following Lemma 5.65) dates back at least to Tarski's 1970 seminar. Lemma 5.66 (except for the final part of (ii)), Lemma 5.72, and Corollary 5.82 date back to Tarski's 1945 seminar and (except for Corollary 5.82) are given in [23]. The same applies to Lemmas 5.75, 5.77, 5.79, and the first dual of Lemma 5.80. Corollary 5.76 (which is the first dual of Lemma 5.75) is implicit in [23]. Corollaries 5.67 and 5.68, and Lemmas 5.69 and 5.70, are from Tarski's 1970 seminar; note however that [23] contains a weaker version of Corollary 5.68 stating that the Boolean product of a set of functions, if it exists, is a function. Lemma 5.74 is due to Monk [86], and Lemma 5.83 to Maddux [72]. A version of Lemma 5.86(ii) is given in Jónsson-Tarski [55], and the implication from right to left in Lemma 5.86(i) is given in Maddux [75]. The remaining parts of Lemma 5.86, as well as Lemma 5.84, Corollary 5.85, and the final part of Lemma 5.66(ii) are due to Andréka and Givant. Lemma 5.73(ii) is due to Givant. Permutations are considered by Tarski [105] under the name *permutational element*; he states that the converse of a permutation is a permutation, and so is the relative product of two permutations. With the help of these observations, Givant formulated and proved Lemma 5.87. The characterization of functions given in Exercise 5.47 is from Chin [22] (see also [23]), while the characterization given in Exercise 5.45 is from Tarski's 1945 seminar, as is the characterization of permutations given in Exercise 5.52. The characterization in Exercise 5.50 of relation algebras in which all atoms are functions is from Jónsson-Tarski [55].

The description implicit in Exercise 5.55 of relations R with the property that $R = R \mid R^{-1} \mid R$ is due to Jacques Riguet [90] and [91]. The result in Exercise 5.53 is from Tarski's 1970 seminar, while the one in Exercise 5.54 is due to Andréka and Givant.

The characterization in Exercise 5.56 of elements that are both functions and equivalence elements is due to Tarski, while the characterization in Exercise 5.57 of elements that are both functions and ideal elements is due to Chin; both results are contained in [22] and [23]. The characterizations in Exercises 5.58–5.65 of elements satisfying various modular laws are all due to Chin and are given in [22] and [23].

Exercises

5.1. Give examples to show that each of the following statements is false.

(i) The relative product of two symmetric elements is symmetric.
(ii) The complement of a transitive element is transitive.
(iii) The sum of two transitive elements is transitive.
(iv) The relative product of two transitive elements is transitive.
(v) The relative sum of two transitive elements is transitive.
(vi) If r, s and $r\,;s$ are all transitive, then $r\,;s = s\,;r$.

5.2. Show that the function ϑ defined on a relation algebra $\mathfrak{A}$ by

$$\vartheta(s) = (-s)^{\smile} \mathbin{+\!\!\!,} s$$

does not in general have the set of all transitive elements in $\mathfrak{A}$ as its range. (Compare this with Lemmas 5.4 and 5.5(vi), and with the next exercise.)

5.3. Prove that the following conditions on an element r are equivalent.

(i) r is reflexive and transitive.
(ii) $r = (-r)^{\smile} \mathbin{+\!\!\!,} r$.
(iii) $r = (-s)^{\smile} \mathbin{+\!\!\!,} s$ for some element s.

5.4. If S is an arbitrary relation in a set relation algebra with base set U, what pairs are in the relation

$$R = S \cap [(\sim S)^{-1} \dagger S]?$$

Show by means of a set-theoretic argument that R must be transitive.

5.5. Prove that a relation R satisfies the equation $R \,|\, R = R$ if and only if R is transitive and dense. (A relation R is said to be *dense* if for every pair (α, β) in R, there is a γ such that (α, γ) and (γ, β) are both in R.)

5.6. Prove that if r and s are transitive, and if

$$\sum_{n=1}^{\infty}(r\,;s)^n \qquad \text{and} \qquad \sum_{n=1}^{\infty}(s\,;r)^n$$

exist, then $\sum_{n=1}^{\infty}(r+s)^n$ exists and

$$\sum_{n=1}^{\infty}(r+s)^n = r+s+\sum_{n=1}^{\infty}(r\,;s)^n + \sum_{n=1}^{\infty}(s\,;r)^n \\ + \Big[\sum_{n=1}^{\infty}(r\,;s)^n\Big]\,;r + r\,;\Big[\sum_{n=1}^{\infty}(s\,;r)^n\Big].$$

5.7. Prove that if r and s are transitive, and $r\,;s = s\,;r$, then

$$\sum_{n=1}^{\infty}(r+s)^n = r + r\,;s + s.$$

5.8. If a relation R satisfies the inequalities

$$R\,|\,R \subseteq R \qquad \text{and} \qquad R\,|\,R^{-1} \subseteq R,$$

is R necessarily an equivalence relation on some set? What if R satisfies the inequalities

$$R\,|\,R \subseteq R \qquad \text{and} \qquad R^{-1}\,|\,R \subseteq R\,?$$

5.9. Prove that the following conditions on an element r are equivalent.

(i) r is reflexive equivalence element.
(ii) $r = [(-r)^{\smile} \mathbin{+\!\!,} r] \cdot (r^{\smile} \mathbin{+\!\!,} -r)$.
(iii) $r = [(-s)^{\smile} \mathbin{+\!\!,} s] \cdot (s^{\smile} \mathbin{+\!\!,} -s)$ for some element s.

5.10. Give a detailed proof that for every element s in a countably complete relation algebra, there is a smallest equivalence element r such that $s \leq r$, and in fact r is given by the equation in Lemma 5.8(ix).

5.11. For an equivalence element r, prove that $r\,;-r = -r\cdot(r\,;1)$.

5.12. For an equivalence element r, prove that

$$(r\,;1+1\,;r)\cdot 1\text{'} \leq r.$$

5.13. If r is a reflexive equivalence element and s an arbitrary element, prove that $r\,;-(r\,;s) = -(r\,;s)$.

5.14. If r is a equivalence element, prove that $r\,;1\,;r$ is also an equivalence element.

5.15. Prove the following generalization of Lemma 5.12: if r and s are equivalence elements, then so is $(r \cdot -s)\,;(r \cdot -s)$. Conclude that if r is an equivalence element, then so are $(r \cdot 0')\,;(r \cdot 0')$ and $-r\,;-r$.

5.16. If r and s are equivalence elements and $r\,;s \leq s$, prove that $r \cdot -s$ is also an equivalence element.

5.17. If r is a equivalence element, prove that

$$r\,;(r \cdot 0') = (r \cdot 0')\,;r$$

and that $r\,;(r \cdot 0')$ is also an equivalence element.

5.18. Determine the non-zero equivalence elements in the complex algebra $\mathfrak{Cm}(P)$ of a geometry P, and show that each such equivalence element is reflexive. Prove that the set of non-zero equivalence elements in $\mathfrak{Cm}(P)$ is a modular lattice with zero and one, under the meet and join operations of Boolean and relative multiplication respectively.

5.19. Determine the non-zero equivalence elements in the complex algebra $\mathfrak{Cm}(L)$ of a modular lattice L with zero, and show that each such equivalence element is reflexive. Prove that the set of non-zero equivalence elements in $\mathfrak{Cm}(L)$ is a modular lattice with zero and one, under the meet and join operations of Boolean and relative multiplication respectively.

5.20. Prove that every modular lattice with zero is isomorphic (as a lattice) to a sublattice of the lattice of non-zero equivalence elements in some abelian relation algebra.

5.21. Prove that $r\,;1 = r\,;r^{\smile}\,;1$ for every element r.

5.22. Prove that for any element r in a relation algebra, the set of all elements below r is a right-ideal if and only if r is a right-ideal element.

5.23. Prove Lemma 5.31 by using Lemmas 5.28–5.30 instead of the inner cylindrification function ϑ.

5.24. Give examples to show that, in general, the set of right-ideal elements in a relation algebra does not contain the identity and diversity elements and is not closed under converse.

5.25. Prove that if r and $s^{\smile}$ are right-ideal elements, then

$$r\,;s = r\cdot s \qquad \text{and} \qquad r \mathbin{\underset{,}{+}} s = r+s.$$

5.26. Prove the following stronger version of Lemma 5.39(ii): if X is a set of subidentity elements, then the sum $\sum X$ exists if and only if the sum $\sum\{1\,;x\,;1 : x\in X\}$ exists, and if one of these sums exists, then

$$1\,;(\sum X)\,;1 = \sum\{1\,;x\,;1 : x\in X\}.$$

In particular, if $r = 1\,;x\,;1$ and $y = 1\,;y\,;1$, then $r+s = 1\,;(x+y)\,;1$.

5.27. Give an example to show that the following improvement of Lemma 5.39(iii) is false: if x and y are subidentity elements, and

$$r = 1\,;x\,;1 \qquad \text{and} \qquad s = 1\,;y\,;1,$$

then $r\cdot s = 1\,;(x\cdot y) : 1$.

5.28. Give an example to show that the following improvement of Lemma 5.39(iv) is false: if x is a subidentity element, and $r = 1\,;x\,;1$, then $-r = 1\,;(1\text{'} - x)\,;1$.

5.29. Give a careful proof of Lemma 5.40.

5.30. Prove Lemma 5.44 by using the modular law for equivalence elements in Lemma 5.14 instead of the modular laws for right- and left-ideal elements.

5.31. Formulate the first dual of Lemma 5.44. What do you notice?

5.32. Formulate the second dual of Lemma 5.44 and prove it directly, without using Lemma 5.44.

5.33. Formulate the second dual of Lemma 5.45 and prove it directly, without using Lemma 5.45.

5.34. Prove that the following conditions on an element r are equivalent.

(i) r is an ideal element.
(ii) $r = r^{\smile} = r\,;r = r \mathbin{\underset{,}{+}} r$.
(iii) r and $-r$ are both equivalence elements.

5.35. Prove for any element r that

$$r\,;1 = 1 \qquad \text{if and only if} \qquad 1\text{'} \le r\,;r^{\smile}.$$

This law gives two equivalent ways of expressing that the domain of a relation is the entire base set.

5.36. Prove that for any subsets X and Y of a set U,

$$id_X \,|(U \times U)\,|\, id_Y = X \times Y.$$

Conclude that a relation R on a set U satisfies the abstract definition for being a rectangle in $\mathfrak{Re}(U)$ if and only if R is a rectangle in the set-theoretic sense of the word.

5.37. Suppose $(x_i : i \in I)$ and $(y_i : i \in I)$ are systems of subidentity elements, and $(r_i : i \in I)$ is a system of arbitrary elements, such that the products

$$\textstyle\prod_i x_i, \qquad \prod_i y_i, \qquad \prod_i r_i$$

all exist. Prove that the product $\prod_i (x_i\,;r_i\,;y_i)$ exists and

$$\textstyle\prod_i (x_i\,;r_i\,;y_i) = (\prod_i x_i)\,;(\prod_i r_i)\,;(\prod_i y_i).$$

5.38. Show that in a non-simple relation algebra, there may exist non-zero subidentity elements x, y, u, and v with $x \ne u$ and $y \ne v$ such that the rectangles $x\,;1\,;y$ and $u\,;1\,;v$ are equal.

5.39. Prove that a square $x\,;1\,;x$ is zero if and only if the side x is zero.

5.40. Prove that a relation R on a set U satisfies the equation

$$R^{-1} \,|\, R \subseteq id_U$$

if and only if R is a function in the set-theoretical sense of the word, that is to say, if and only if the presence of pairs (α, β) and (α, γ) in R always implies that $\beta = \gamma$.

5.41. Determine which elements are functions in the complex algebra of a group.

5.42. Determine which elements are functions in the complex algebra of a geometry.

5.43. Give an example to show that the hypothesis of disjointness in Lemma 5.72 cannot be dropped.

5.44. Formulate the first dual of Lemma 5.77.

5.45. Prove that r is a function if and only if

$$(r^{\smile} ; s) - t = r^{\smile} ; [s - (r ; t)]$$

for all elements s and t.

5.46. Formulate the first dual of the law in Exercise 5.45.

5.47. Prove that r is a function if and only if the modular law

$$r ; [s \,+\!\!\!\!,\, (r ; t)] = (r ; s) \,+\!\!\!\!,\, (r ; t)$$

holds for all elements s and t.

5.48. Prove that if r is a function, then $r;r^{\smile}$ is an equivalence element.

5.49. If r is a function and $r ; 1 = 1$, prove that $-(r ; s) = r ; -s$ for every element s.

5.50. Prove that in a relation algebra, the following conditions are equivalent.

(i) Every atom is a function.
(ii) If r and s are atoms, then $r ; s = 0$ or $r ; s$ is an atom.
(iii) If r is an atom, then so is $r^{\smile} ; r$.

5.51. Prove that if r and s are bijections, then so is $r ; s$.

5.52. Prove that r is a permutation if and only if

$$r^{\smile} ; r = 1' \qquad \text{and} \qquad r ; r^{\smile} = 1'.$$

5.53. Prove that if r is either a function, an equivalence element, a right-ideal element, or a left-ideal element, then $r = r ; r^{\smile} ; r$.

5.54. Prove that if r satisfies the equation $r = r ; r^{\smile} ; r$, then $r^{\smile} ; r$ and $r ; r^{\smile}$ are equivalence elements.

5.55. Describe the relations R in a full set relation algebra $\mathfrak{Re}(U)$ with the property that $R = R \mid R^{-1} \mid R$.

5.56. Prove that r is a function and an equivalence element if and only if r is a subidentity element.

5.57. Prove that the following conditions on an element r are equivalent.

(i) r is a function and an ideal element.
(ii) r is a function and a right-ideal element.
(iii) $1 \mathbin{;} r \mathbin{;} 1 \leq 1'$.
(iv) $r \mathbin{;} 1 \leq 1'$.

5.58. Prove that the following conditions on an element r are equivalent.

(i) $r = 1$.
(ii) $r \cdot (s + t) = r \cdot s + t$ for all elements s and t.
(iii) $r \cdot (s \mathbin{\underset{,}{+}} t) = r \cdot s \mathbin{\underset{,}{+}} t$ for all elements s and t.

5.59. Prove that $r \mathbin{;} (s + t) = r \mathbin{;} s + t$ for all elements s and t if and only if $r = 1'$.

5.60. Prove that $r \mathbin{;} (s \cdot t) = (r \mathbin{;} s) \cdot t$ for all elements s and t if and only if $r \leq 1'$.

5.61. Prove that $r \mathbin{;} (s \mathbin{\underset{,}{+}} t) = r \mathbin{;} s \mathbin{\underset{,}{+}} r \mathbin{;} t$ for all elements s and t if and only if $r = (1 \mathbin{;} r \mathbin{;} 1) \cdot 1'$.

5.62. Prove that $s \cdot (r \mathbin{;} t) = (s \cdot r) \mathbin{;} t$ for all elements s and t if and only if $1 \mathbin{;} r \mathbin{;} 1 \leq 1'$.

5.63. Prove that $r \cdot [s \mathbin{;} (r \cdot t)] = (r \cdot s) \mathbin{;} (r \cdot t)$ for all elements s and t if and only if $r \mathbin{;} r \leq r$ and $r \mathbin{;} r^{\smile} \leq r$.

5.64. Prove that $r \mathbin{;} [s \cdot (r \mathbin{;} t)] = (r \mathbin{;} s) \cdot (r \mathbin{;} t)$ for all elements s and t if and only if $r \mathbin{;} r \leq r$ and $r^{\smile} \mathbin{;} r \leq r$.

5.65. Prove that $r \mathbin{;} [s + (r \mathbin{;} t)] = (r \mathbin{;} s) + (r \mathbin{;} t)$ for all elements s and t if and only if $r \mathbin{;} r = r$.

Chapter 6
Subalgebras

There are several general algebraic methods for constructing new relation algebras from old ones. Among them are the formation of subalgebras, quotients, and direct products. In this chapter we focus on those methods that are connected with the formation of various kinds of subalgebras. Quotients and direct products will be discussed in Chapters 8 and 11 respectively.

6.1 Subuniverses and subalgebras

Consider an algebra

$$\mathfrak{A} = (A\,,\,+\,,\,-\,,\,;\,,\,\smile\,,\,1\text{'})$$

of the same similarity type as relation algebras. A *subuniverse* of $\mathfrak{A}$ is defined to be a subset B of the universe A that contains the element 1' and is *closed under the operations* of $\mathfrak{A}$ in the sense that if r and s are elements in B, then so are

$$r + s, \qquad -r, \qquad r\,;s, \qquad \text{and} \qquad r^{\smile}.$$

Every subuniverse of $\mathfrak{A}$ must contain the distinguished elements 0, 1, and 0' in $\mathfrak{A}$, and must be closed under the operations of multiplication and relative addition in $\mathfrak{A}$, because these elements and operations are defined by means of terms in $\mathfrak{A}$.

A *subalgebra* of $\mathfrak{A}$ is a subuniverse B of $\mathfrak{A}$, together with the distinguished element of $\mathfrak{A}$ and the restrictions of the operations of $\mathfrak{A}$ to the set B as its fundamental operations. If $\mathfrak{B}$ is a subalgebra of $\mathfrak{A}$, then $\mathfrak{A}$

S. Givant, *Introduction to Relation Algebras*,
DOI 10.1007/978-3-319-65235-1_6

is called an *extension* of $\mathfrak{B}$. It is common practice—one that we shall often follow—to identify subuniverses with the corresponding subalgebras, and therefore to speak of subalgebras as if one were speaking of subuniverses, and vice versa. For example, we write $\mathfrak{B} \subseteq \mathfrak{A}$ or $\mathfrak{A} \supseteq \mathfrak{B}$ to express that $\mathfrak{B}$ is a subalgebra of $\mathfrak{A}$, and we shall sometimes say that $\mathfrak{B}$ is *included in* $\mathfrak{A}$, or that $\mathfrak{A}$ *includes* $\mathfrak{B}$.

Every relation algebra $\mathfrak{A}$ has a largest subalgebra, namely $\mathfrak{A}$ itself. It is called the *improper* subalgebra of $\mathfrak{A}$. Every other subalgebra of $\mathfrak{A}$ is said to be a *proper* subalgebra.

The relation of being a subalgebra has several important and easily verified properties. First, it is reflexive in the sense that every algebra is a subalgebra of itself. Second, it is antisymmetric in the sense that if two algebras are subalgebras of each other, then they must be equal. Finally, it is transitive in the sense that if $\mathfrak{B}$ is a subalgebra of $\mathfrak{A}$, and $\mathfrak{C}$ a subalgebra of $\mathfrak{B}$, then $\mathfrak{C}$ must be a subalgebra of $\mathfrak{A}$. Thus, the relation of being a subalgebra is a partial order on the class of all relation algebras, and indeed on the class of all algebras. We shall return to this point in Section 6.4.

The equational nature of axioms (R1)–(R10) implies that every subalgebra of a relation algebra is again a relation algebra. In more detail, if $\mathfrak{B}$ is a subalgebra of a relation algebra $\mathfrak{A}$, and if r, s, and t are elements in $\mathfrak{B}$, then these elements also belong to $\mathfrak{A}$, and therefore the equations in (R1)–(R10) hold for these elements in $\mathfrak{A}$. Since the operations of $\mathfrak{B}$ are just restrictions to B of the operations in $\mathfrak{A}$, it follows that the equations hold for these elements in $\mathfrak{B}$ as well, so $\mathfrak{B}$ is a relation algebra.

6.2 Properties preserved under subalgebras

The observation made above that subalgebras of relation algebras are relation algebras is a special case of a much more general phenomenon: the passage to a subalgebra preserves all algebraic properties that are expressible by means of universal formulas. To prove this statement, it is helpful to formulate a lemma concerning the preservation of values of terms under the passage to subalgebras.

Lemma 6.1. *If $\mathfrak{B}$ is a subalgebra of $\mathfrak{A}$, then for every term γ and every appropriate sequence r of elements in $\mathfrak{B}$, the value of $\gamma(r)$ is the same in $\mathfrak{B}$ as it is in $\mathfrak{A}$.*

Proof. The proof proceeds by induction on terms. There are two base cases to consider. If γ is a variable v_i, then the value of $\gamma(r)$ is r_i in both $\mathfrak{B}$ and $\mathfrak{A}$, so the conclusion of the lemma holds. If γ is the individual constant symbol 1', then the value of $\gamma(r)$ is the identity element in $\mathfrak{B}$ and in $\mathfrak{A}$, and these two identity elements are the same, by the assumption that $\mathfrak{B}$ is a subalgebra of $\mathfrak{A}$. Consequently, the conclusion of the lemma holds in this case as well.

Assume now as the induction hypothesis that σ and τ are terms such that the value of $\sigma(r)$ is the same in $\mathfrak{B}$ as it is in $\mathfrak{A}$, and similarly for $\tau(r)$. There are four cases to consider. If γ is the term $\sigma ; \tau$, then

$$\begin{aligned} \gamma^{\mathfrak{B}}(r) = (\sigma ; \tau)^{\mathfrak{B}}(r) = \sigma^{\mathfrak{B}}(r) ; \tau^{\mathfrak{B}}(r) \\ = \sigma^{\mathfrak{A}}(r) ; \tau^{\mathfrak{A}}(r) = (\sigma ; \tau)^{\mathfrak{A}}(r) = \gamma^{\mathfrak{B}}(r). \end{aligned}$$

The first and last equalities use the assumption on γ, and the second and fourth use the definition of the value of a term on a sequence of elements in an algebra (see Section 2.4). The third equality uses the induction hypotheses on σ and τ, together with the assumption that $\mathfrak{B}$ is a subalgebra of $\mathfrak{A}$, which implies that relative multiplication in $\mathfrak{B}$ is just the restriction of relative multiplication in $\mathfrak{A}$. Thus, the conclusion of the lemma holds in this case. A similar argument applies if γ is one of the terms $\sigma + \tau$, or $-\sigma$, or $\sigma^{\smile}$. Use the principle of induction for terms to arrive at the desired conclusion. □

For equations, and more generally, for quantifier-free formulas Γ, a sequence of elements satisfies Γ in a subalgebra if and only if it satisfies Γ in the parent algebra.

Lemma 6.2. *If $\mathfrak{B}$ is a subalgebra of $\mathfrak{A}$, then for every quantifier-free formula Γ and every appropriate sequence r of elements in $\mathfrak{B}$, the sequence r satisfies Γ in $\mathfrak{B}$ if and only if it satisfies Γ in $\mathfrak{A}$.*

Proof. The proof proceeds by induction on quantifier-free formulas. For the base case, suppose that Γ is an equation, say $\sigma = \tau$. The value of $\sigma(r)$ is the same in $\mathfrak{B}$ as it is in $\mathfrak{A}$, by Lemma 6.1, and similarly for value of $\tau(r)$. Consequently, r satisfies the equation Γ in $\mathfrak{B}$ if and only if it satisfies Γ in $\mathfrak{A}$, by the definition of satisfaction.

Assume now as the induction hypothesis that the lemma holds for formulas Δ and Φ. If Γ is the formula $\neg\Delta$, then the sequence r satisfies Γ in $\mathfrak{B}$ if and only if it does not satisfy Δ in $\mathfrak{B}$, by the definition of satisfaction, and similarly for the algebra $\mathfrak{A}$. The induction hypothesis

implies that r does not satisfy Δ in $\mathfrak{B}$ if and only if r does not satisfy Δ in $\mathfrak{A}$. Combine these observations to conclude that r satisfies Γ in $\mathfrak{B}$ if and only if r satisfies Γ in $\mathfrak{A}$.

If Γ is the formula $\Phi \to \Delta$, then the sequence r satisfies Γ in $\mathfrak{B}$ if and only if it satisfies Δ whenever it satisfies Φ in $\mathfrak{B}$, and similarly for the algebra $\mathfrak{A}$, by the definition of satisfaction. The induction hypothesis implies that r satisfies Δ whenever it satisfies Φ in $\mathfrak{B}$ if and only if r satisfies Δ whenever it satisfies Φ in $\mathfrak{A}$. Combine these observations to conclude, as before, that r satisfies Γ in $\mathfrak{B}$ if and only if r satisfies Γ in $\mathfrak{A}$. Use the principle of induction for open formulas to arrive at the desired conclusion. □

From Lemma 6.2, it may be concluded that for universal formulas, satisfaction is preserved under the passage to appropriate subalgebras.

Corollary 6.3. *If a universal formula Γ is satisfied by a sequence r of elements in an algebra $\mathfrak{A}$, then Γ is satisfied by r in all subalgebras of $\mathfrak{A}$ that contain the elements of r.*

Proof. Suppose Γ has the form

$$\forall v_0 \ldots \forall v_{m-1} \Delta(v_0, \ldots v_{m-1}, v_m, \ldots, v_{n-1}),$$

where Δ is a quantifier-free formula (and $0 \le m \le n$), and consider a sequence

$$r = (r_m, \ldots, r_{n-1}) \tag{1}$$

of elements that satisfies Γ in $\mathfrak{A}$. The definition of satisfaction implies that for any elements $r_0, \ldots, r_{m-1}$ in $\mathfrak{A}$, the sequence

$$(r_0, \ldots, r_{m-1}, r_m, \ldots, r_{n-1}) \tag{2}$$

satisfies Δ in $\mathfrak{A}$. Let $\mathfrak{B}$ be any subalgebra of $\mathfrak{A}$ that contains the elements of (1), and consider any m elements $r_0, \ldots, r_{m-1}$ in $\mathfrak{B}$. These elements all belong to $\mathfrak{A}$, because $\mathfrak{B}$ is a subalgebra of $\mathfrak{A}$. Consequently, the resulting sequence (2) satisfies Δ in $\mathfrak{A}$, by the preceding remarks. Since Δ is assumed to be a quantifier-free formula, the sequence (2) must also satisfy Δ in $\mathfrak{B}$, by Lemma 6.2. This is true for any m elements in $\mathfrak{B}$, so the definition of satisfaction implies that the sequence (1) satisfies Γ in $\mathfrak{B}$. □

Corollary 6.4. *If a universal formula Γ is true in an algebra $\mathfrak{A}$, then Γ is true in all subalgebras of $\mathfrak{A}$.*

We say that a property of algebras is *preserved under subalgebras* if it is inherited by all subalgebras of an algebra that possesses the property. Similarly, a property of elements, or of sequences of elements, is said to be preserved under subalgebras if whenever the property holds for an element (or a sequence of elements) r in an algebra $\mathfrak{A}$, then it holds for r in every subalgebra of $\mathfrak{A}$ that contains r (or the elements in r). It follows at once from Lemma 6.2 that all properties of elements that are defined by equations are preserved under the passage to subalgebras. This applies in particular to all of the properties that are discussed in Chapter 5. Thus, for example, if $\mathfrak{B}$ is a subalgebra of a relation algebra $\mathfrak{A}$, then an element r in $\mathfrak{B}$ is an equivalence element, or an ideal element, or a rectangle, or a function, or the domain of an element s, in $\mathfrak{B}$ if and only if r has this same property in $\mathfrak{A}$. In a similar vein, it follows from Corollary 6.4 that if $\mathfrak{A}$ is an abelian or a symmetric relation algebra, then so is every subalgebra of $\mathfrak{A}$. In Chapter 9, we shall see two more very important and non-trivial examples of properties of relation algebras that are preserved under subalgebras, namely the property of being simple and the property of being integral.

It also follows from Lemmas 6.1 and 6.2 that all operations and relations on the universe of a relation algebra that are definable by means of universal formulas are preserved under the passage to subalgebras. For example, the operation of relative addition is defined by a term, so if r and s are elements in a subalgebra $\mathfrak{B}$ of a relation algebra $\mathfrak{A}$, then the relative sum of r and s is the same in $\mathfrak{B}$ as it is in $\mathfrak{A}$. Similarly, the partial order $\leq$ is defined by an equation, so if r and s are elements in the subalgebra $\mathfrak{B}$, then $r \leq s$ holds in $\mathfrak{B}$ if and only if it holds in $\mathfrak{A}$.

6.3 Generators of subalgebras

The intersection of every system of subalgebras of $\mathfrak{A}$ is again a subalgebra of $\mathfrak{A}$. Indeed, if r and s are elements in the intersection $\mathfrak{B}$ of a system $(\mathfrak{B}_i : i \in I)$ of subalgebras of $\mathfrak{A}$, then r and s belong to $\mathfrak{B}_i$ for every i, and therefore so do the sum and relative product of r and s, and the complement and converse of r. Consequently, all of these elements belong to the intersection $\mathfrak{B}$. A similar argument shows that 1' belongs to $\mathfrak{B}$, so $\mathfrak{B}$ is a subalgebra of $\mathfrak{A}$.

The intersection $\mathfrak{B}$ is in fact the largest subalgebra of $\mathfrak{A}$ that is included in each subalgebra $\mathfrak{B}_i$ in the system. Indeed, if $\mathfrak{C}$ is a subalgebra of $\mathfrak{A}$ that is included in $\mathfrak{B}_i$ for each i, then $\mathfrak{C}$ must be included in the intersection, by the definition of the intersection. For this reason, the intersection of the system is also called the *infimum*, or the *meet*, of the given system of subalgebras. The special case when the system of subalgebras is empty is worth discussing for a moment, if only to avoid later confusion. The improper subalgebra $\mathfrak{A}$ is vacuously included in every subalgebra in the empty system (there is no subalgebra in the empty system that does not include $\mathfrak{A}$), and it is clearly the largest subalgebra with this property. Consequently, $\mathfrak{A}$ is, by definition, the infimum of the empty system of subalgebras.

It follows from the preceding remarks that if X is a subset of $\mathfrak{A}$, then the intersection of all those subalgebras of $\mathfrak{A}$ that include X is a subalgebra. (There is always at least one subalgebra that includes X, namely the improper subalgebra $\mathfrak{A}$.) That intersection, say $\mathfrak{B}$, is the smallest subalgebra of $\mathfrak{A}$ that includes X; in other words, $\mathfrak{B}$ includes X, and $\mathfrak{B}$ is included in every subalgebra of $\mathfrak{A}$ that includes X (because every such subalgebra of $\mathfrak{A}$ is, by definition, one of the subalgebras in the system whose intersection is defined to be $\mathfrak{B}$). The subalgebra $\mathfrak{B}$ is said to be *generated by* X, and X is called a *set of generators* of $\mathfrak{B}$. A simple but useful remark for subsets X and Y of $\mathfrak{A}$ is that whenever X is included in Y, the subalgebra generated by X is included in the subalgebra generated by Y. Indeed, every subalgebra of $\mathfrak{A}$ that includes Y also includes X; consequently, the intersection of the system of subalgebras of $\mathfrak{A}$ that include Y is an extension of the intersection of the system of subalgebras of $\mathfrak{A}$ that include X. In particular, the subalgebra generated by the empty set is included in every subalgebra of $\mathfrak{A}$. It is called the *minimal subalgebra* of $\mathfrak{A}$. A relation algebra $\mathfrak{A}$ is said to be *finitely generated* if it is generated by some finite subset.

The preceding definition of the subalgebra generated by a set of elements is top-down and non-constructive. It gives no idea of the elements that actually belong to the subalgebra. There is a bottom-up approach that gives more precise information about these elements. Fix an arbitrary subset X of a relation algebra $\mathfrak{A}$, and define a system of subsets X_i of $\mathfrak{A}$ by induction on natural numbers i. The set X_0 is defined to be $X \cup \{1'\}$, and if X_i has been defined, then X_{i+1} is defined to be the set of all elements

$$r + s, \qquad -r, \qquad r \,;\, s, \qquad r^{\smile},$$

where r and s vary over elements in X_i. The set X_{i+1} is called the *one-step closure* of the set X_i.

Lemma 6.5. *Each set X_i is included in the set X_{i+1}, and the union of these sets, $B = \bigcup_i X_i$, is the smallest subuniverse of $\mathfrak{A}$ that includes the set X.*

Proof. To prove that X_i is included in X_{i+1}, observe that if r is any element in X_i, then the sum $r + r$ belongs to X_{i+1}, by the definition of this set. Since this sum is just r, it follows that r belongs to X_{i+1}.

The next step is to prove that the union set B is a subuniverse of $\mathfrak{A}$ that includes X. Indeed, X is included in B because X is included in X_0, and 1' belongs to B for the same reason. Assume now that r and s are elements in B. Since B is the union of the sets X_i, there must be natural numbers i and j such that r is in X_i and s in X_j. Without loss of generality, it may be assumed that $i \le j$. In this case, r belongs to X_j, because X_i is included in X_j, and therefore the elements

$$r + s, \qquad -r, \qquad r\,;s, \qquad \text{and} \qquad r^{\smile}$$

all belong to the set X_{j+1}, by the definition of this set. Consequently, these elements all belong to B, so B is closed under the operations of $\mathfrak{A}$ and is therefore a subuniverse of $\mathfrak{A}$.

Finally, to show that B is the smallest subuniverse that includes X, consider any subuniverse C of $\mathfrak{A}$ that includes X. A simple argument by induction on i shows that X_i is included in C for each natural number i. Indeed, X_0 is included in C because X is assumed to be included in C and because 1' belongs to C. If X_i is included in C, then the sums, complements, relative products, and converses of all the elements in X_i must also belong to C, because C is closed under the operations of $\mathfrak{A}$. Consequently, the set X_{i+1} must be included in C, by the definition of this set. Since each set X_i is included in C, the union $\bigcup_i X_i$, which is B, is also included in C. Conclusion: the set B is included in every subuniverse of $\mathfrak{A}$ that includes X, so B is the smallest subuniverse of $\mathfrak{A}$ that includes X. □

One consequence of the preceding lemma is that it places an upper bound on the size of the subalgebra generated by a given set X.

Corollary 6.6. *If a subset X of a relation algebra is finite, then the subalgebra generated by X is countable. If X is infinite, then the subalgebra generated by X has the same cardinality as X.*

Every finitely generated Boolean algebra is finite, and in fact it is isomorphic to the Boolean algebra of all subsets of some finite set. In particular, every finite Boolean algebra has cardinality 2^n for some natural number n. It follows that every finite relation algebra must have cardinality 2^n for some natural number n, because the Boolean part of a finite relation algebra is a finite Boolean algebra. It is not true, however, that every finitely generated relation algebra is finite. There are in fact infinite relation algebras that are generated by a single element. Consider for example the set $\mathbb{N}$ of all natural numbers, and let $\mathfrak{A}$ be the full set relation algebra on $\mathbb{N}$. The successor relation R in $\mathfrak{A}$ that is defined by

$$R = \{(n, n+1) : n \in \mathbb{N}\}$$

generates an infinite subalgebra of $\mathfrak{A}$. In fact, a straightforward induction on natural numbers m shows that the mth power of R is the relation

$$R^m = \{(n, n+m) : n \in \mathbb{N}\},$$

and these relations are all distinct for distinct natural numbers m.

The problem of describing all finitely generated relation algebras is impossibly difficult. It is known, for example, that there is a relation algebra $\mathfrak{A}$ with one generator such that all of set theory can be encoded into $\mathfrak{A}$ (see [113]), so the problem of describing relation algebras with a single generator is as difficult as the problem of describing all sets.

6.4 Lattice of subalgebras

The relation of one subalgebra being included in another is a partial order on the set of subalgebras of $\mathfrak{A}$ (see the relevant remarks in Section 6.1), and under this partial order the set of subalgebras of $\mathfrak{A}$ becomes a complete lattice. The infimum, or meet, of a system of subalgebras is the intersection of the system. The supremum, or join, of the system is the subalgebra generated by the set that is the union of the universes of the subalgebras in the system. In other words, the join is the smallest subalgebra that includes every member of the system as a subalgebra. The zero of the lattice is the minimal subalgebra, and the unit is the improper subalgebra.

In general, the join of a system of subalgebras is not the union of the system, because that union is usually not a subalgebra. There is

an exception, however. A system $(\mathfrak{A}_i : i \in I)$ of algebras is said to be *directed* if any two members $\mathfrak{A}_i$ and $\mathfrak{A}_j$ of the system are always subalgebras of some third member $\mathfrak{A}_k$.

Lemma 6.7. *The union of a non-empty, directed system of subalgebras of a relation algebra $\mathfrak{A}$ is again a subalgebra of $\mathfrak{A}$.*

Proof. Let $(\mathfrak{B}_i : i \in I)$ be a non-empty, directed system of subalgebras of $\mathfrak{A}$, and let B be the union of the universes of the algebras in the system. It is to be shown that B is a subuniverse of $\mathfrak{A}$. Certainly, the identity element 1' belongs to B, since it belongs to each member of the directed system, and the system is assumed to be non-empty. To show that B is closed under the operations of $\mathfrak{A}$, consider elements r and s in B. There must be indices i and j in I such that r is in $\mathfrak{B}_i$ and s in $\mathfrak{B}_j$, by the definition of B. These two subalgebras are included in some third subalgebra $\mathfrak{B}_k$ of the system, because the system is assumed to be directed. The elements r and s are therefore both in $\mathfrak{B}_k$, and consequently so are their sum, complements, relative product, and converses. It follows that the sum, complements, relative product, and converses of r and s also belong to B, as desired. $\square$

The lemma applies, in particular, to non-empty systems of subalgebras that are linearly ordered by the relation of being a subalgebra. Such systems are called *chains*.

Corollary 6.8. *The union of a non-empty chain of subalgebras of a relation algebra $\mathfrak{A}$ is again a subalgebra of $\mathfrak{A}$.*

Lemma 6.7 implies that every relation algebra is the union of a directed system of finitely generated subalgebras. To prove this, we begin with a more general lemma.

Lemma 6.9. *Suppose a relation algebra $\mathfrak{A}$ is generated by a set X. For each finite subset Y of X, let $\mathfrak{A}_Y$ be the subalgebra of $\mathfrak{A}$ generated by Y. The system of subalgebras*

$$(\mathfrak{A}_Y : Y \subseteq X \textit{ and } Y \textit{ is finite})$$

is directed, and its union is $\mathfrak{A}$.

Proof. The given system is easily seen to be directed. Indeed, if Y_1 and Y_2 are finite subsets of X, then so is the set $Y = Y_1 \cup Y_2$, and the subalgebras generated by Y_1 and Y_2 are both included in the subalgebra

generated by Y. It follows from Lemma 6.7 that the union of this directed system is a subalgebra of $\mathfrak{A}$. Since this union includes every finite subset of X, it must include X itself, and therefore the union must include the subalgebra generated by X, which is $\mathfrak{A}$. □

Take the universe of $\mathfrak{A}$ for the set X in the preceding lemma to arrive at the desired conclusion.

Corollary 6.10. *Every relation algebra is the union of a directed system of finitely generated subalgebras.*

An element in a lattice is said to be *compact* if it has the following property: whenever it is below the join of a system of elements in the lattice, then it is below the join of a finite subsystem of these elements.

Lemma 6.11. *Finitely generated subalgebras are compact in the lattice of subalgebras of a relation algebra.*

Proof. We begin with a preliminary observation. Suppose $\mathfrak{B}$ is the join of a system

$$(\mathfrak{B}_i : i \in I) \tag{1}$$

of subalgebras of a relation algebra $\mathfrak{A}$. Write X for the union of the universes of the subalgebras in the system, and observe that X generates $\mathfrak{B}$, by the definition of the join of a system of subalgebras. Apply Lemma 6.9 to see that $\mathfrak{B}$ is the union of the directed system of subalgebras generated by the finite subsets of X. It follows that every element in $\mathfrak{B}$ belongs to a subalgebra generated by some finite subset of X.

Consider now a finitely generated subalgebra $\mathfrak{C}$ of $\mathfrak{A}$, and let Z be a finite set of generators of $\mathfrak{C}$. To establish the compactness of $\mathfrak{C}$, suppose that $\mathfrak{C}$ is a subalgebra of the join of a system (1) of subalgebras of $\mathfrak{A}$. Take X be the union of the universes of these subalgebras, as before. Each element r in the set Z is generated by a finite subset Y_r of X, by the observation of the first paragraph. Let Y be the union of the sets Y_r for r in Z. As a union of finitely many finite sets, Y must be a finite subset of X. Also, Y generates the elements in Z, and Z generates $\mathfrak{C}$, so $\mathfrak{C}$ must be included in the subalgebra of $\mathfrak{A}$ generated by Y.

Each element in Y belongs to the set X, which is defined to be the union of the universes of the subalgebras in system (1), so each element in Y belongs to some subalgebra $\mathfrak{B}_i$ in (1). Since Y is finite, there must be a finite subset J of the index set I such that Y is included in the

union of the universes of the subsystem $(\mathfrak{B}_i : i \in J)$, and therefore also in the join of this subsystem . Consequently, the subalgebra generated by Y is included in the join of this subsystem. Since $\mathfrak{C}$ is included in the subalgebra generated by Y, it must be included in the join of the subsystem as well. $\square$

Lemmas 6.9 and 6.11 imply that every subalgebra of a relation algebra $\mathfrak{A}$ is the join of compact elements. Lattices with this property are said to be *compactly generated*. The following theorem has been proved.

Theorem 6.12. *The subalgebras of a relation algebra form a complete, compactly generated lattice that is closed under directed unions.*

The lattice structure gives a rough classification of the subalgebras of a relation algebra: the structurally less complicated subalgebras are toward the bottom of the lattice, and the structurally more complicated subalgebras are toward the top.

The notion of a directed system of algebras makes sense even if the algebras in the system are not assumed *a priori* all to be subalgebras of some given algebra. Moreover, the union of such a system always exists. Indeed, given a system $(\mathfrak{A}_i : i \in I)$ of algebras, define the *union* of the system to be the algebra $\mathfrak{A}$ determined as follows. The universe of $\mathfrak{A}$ is the union of the universes of the algebras in the system. For any two elements r and s in $\mathfrak{A}$, there are indices i and j such that r is in $\mathfrak{A}_i$ and s in $\mathfrak{A}_j$. The assumption that the system is directed implies that there is an index k such that $\mathfrak{A}_i$ and $\mathfrak{A}_j$ are subalgebras of $\mathfrak{A}_k$. In particular, r and s both belong to $\mathfrak{A}_k$. The sum and relative product of r and s, and the complement and converse of r, in the union $\mathfrak{A}$ are respectively defined to be the sum and relative product of r and s, and the complement and converse of r, in $\mathfrak{A}_k$. The identity element in $\mathfrak{A}$ is defined to be the identity element in any one of the algebras of the directed system. These definitions are independent of the choice of the algebra $\mathfrak{A}_k$ (as well as the algebras $\mathfrak{A}_i$ and $\mathfrak{A}_j$). For example, if r and s both belong to some other algebra $\mathfrak{A}_\ell$ in the system, then there is an index m such that $\mathfrak{A}_k$ and $\mathfrak{A}_\ell$ are both subalgebras of $\mathfrak{A}_m$. The relative product of r and s in $\mathfrak{A}_k$ and in $\mathfrak{A}_\ell$ must therefore be equal, because they are both equal to the relative product of r and s in $\mathfrak{A}_m$. The same remark applies to the other operations and to the identity element. Analogous arguments show that every algebra $\mathfrak{A}_i$ in the directed system is a subalgebra of the union $\mathfrak{A}$, and that a relation

algebraic equation is valid in $\mathfrak{A}$ if and only if it is valid in each algebra of the directed system. We summarize these observations in the following lemma.

Lemma 6.13. *The union of a non-empty directed system of relation algebras is a relation algebra that is an extension of every algebra in the system.*

A special case of the lemma occurs when the directed system of algebras is in fact a chain in the sense that it is linearly ordered by the relation of being a subalgebra.

Corollary 6.14. *The union of a non-empty chain of relation algebras is a relation algebra that is an extension of every algebra in the chain.*

6.5 Regular and complete subalgebras

If $\mathfrak{B}$ is a subalgebra of a complete relation algebra $\mathfrak{A}$, and if the supremum in $\mathfrak{A}$ of every subset of $\mathfrak{B}$ belongs to $\mathfrak{B}$, then $\mathfrak{B}$ is called a *complete subalgebra* of $\mathfrak{A}$. Equivalently, $\mathfrak{B}$ is a complete subalgebra of $\mathfrak{A}$ just in case the infimum in $\mathfrak{A}$ of every subset of $\mathfrak{B}$ belongs to $\mathfrak{B}$. Consequently, a complete subalgebra $\mathfrak{B}$ contains the infima and suprema of all of its subsets, and these infima and suprema are the same in $\mathfrak{B}$ as they are in $\mathfrak{A}$. In particular, a complete subalgebra is a complete relation algebra. The universe of a complete subalgebra of $\mathfrak{A}$ is called a *complete subuniverse* of $\mathfrak{A}$.

For a complete relation algebra $\mathfrak{A}$, the complete subalgebra *generated* by a subset X is defined to be the intersection of the complete subalgebras of $\mathfrak{A}$ that include X. It is not difficult to check that this intersection is a complete subalgebra of $\mathfrak{A}$, and in fact it is the smallest complete subalgebra of $\mathfrak{A}$ that includes X. We shall sometimes say that this subalgebra is *completely generated* by X.

There is an intermediate notion, stronger than “subalgebra”, but weaker than “complete subalgebra”, that is sometimes useful. It does not require the algebra $\mathfrak{A}$ to be complete. To motivate it, we make a preliminary obvious, but useful, observation.

Lemma 6.15. *Suppose* $\mathfrak{B}$ *is a subalgebra of* $\mathfrak{A}$, *and* X *a subset of* $\mathfrak{B}$. *If an element* r *in* $\mathfrak{B}$ *is the supremum of* X *in* $\mathfrak{A}$, *then* r *remains the supremum of* X *in* $\mathfrak{B}$, *in symbols*,

$$r = \sum\nolimits^{\mathfrak{A}} X \qquad \textit{implies} \qquad r = \sum\nolimits^{\mathfrak{B}} X.$$

The requirement that $\mathfrak{B}$ be a regular subalgebra of $\mathfrak{A}$ is just the reverse implication. A *regular subalgebra* of a relation algebra $\mathfrak{A}$ is defined to be a subalgebra $\mathfrak{B}$ with the following additional property: for all subsets X of $\mathfrak{B}$, if X has a supremum r in $\mathfrak{B}$, then X has a supremum in $\mathfrak{A}$ as well, and that supremum is r. (Warning: a subset of $\mathfrak{B}$ may have a supremum in $\mathfrak{A}$ without having a supremum in $\mathfrak{B}$; the definition says nothing about such subsets.) Intuitively, this definition says that all suprema which exist in the subalgebra $\mathfrak{B}$ are preserved in the passage to the extension $\mathfrak{A}$. If $\mathfrak{B}$ is a regular subalgebra of $\mathfrak{A}$, then $\mathfrak{A}$ is called a *regular extension* of $\mathfrak{B}$. In a complete relation algebra $\mathfrak{A}$, complete subalgebras are always regular subalgebras, but the reverse implication may fail; that is to say, there may be regular subalgebras of $\mathfrak{A}$ that are not complete subalgebras. If, however, $\mathfrak{B}$ is a regular subalgebra of $\mathfrak{A}$, and $\mathfrak{B}$ is complete, then $\mathfrak{B}$ must be a complete subalgebra of $\mathfrak{A}$.

Just as the notion of subalgebra is transitive, so too the notion of a regular subalgebra is transitive, and in fact it is *strongly transitive* in the sense of the following lemma.

Lemma 6.16. (i) *If* $\mathfrak{C}$ *is a regular subalgebra of* $\mathfrak{B}$, *and* $\mathfrak{B}$ *is a regular subalgebra of* $\mathfrak{A}$, *then* $\mathfrak{C}$ *is a regular subalgebra of* $\mathfrak{A}$.

(ii) *If* $\mathfrak{C}$ *is a regular subalgebra of* $\mathfrak{A}$, *and* $\mathfrak{B}$ *is a subalgebra of* $\mathfrak{A}$ *that includes* $\mathfrak{C}$, *then* $\mathfrak{C}$ *is a regular subalgebra of* $\mathfrak{B}$.

Proof. Consider a subset X of $\mathfrak{C}$ that has a supremum r in $\mathfrak{C}$. If the hypotheses of (i) hold, then r must be the supremum of X in $\mathfrak{B}$, by the assumption that $\mathfrak{C}$ is a regular subalgebra of $\mathfrak{B}$, and consequently r must be the supremum of X in $\mathfrak{A}$, by the the assumption that $\mathfrak{B}$ is a regular subalgebra of $\mathfrak{A}$. It follows that $\mathfrak{C}$ is a regular subalgebra of $\mathfrak{A}$. This proves (i)

On the other hand, if the hypotheses of (ii) hold, then r must be the supremum of X in $\mathfrak{A}$, because $\mathfrak{C}$ is assumed to be a regular subalgebra of $\mathfrak{A}$. Since $\mathfrak{C}$ is a subalgebra of $\mathfrak{B}$, by assumption, the set X is included in $\mathfrak{B}$, and r is an element in $\mathfrak{B}$. It follows that r, being the supremum of X in $\mathfrak{A}$, must also be the supremum of X in $\mathfrak{B}$, by Lemma 6.15. Thus, $\mathfrak{C}$ is a regular subalgebra of $\mathfrak{B}$. This proves (ii). □

A necessary and sufficient condition for a subalgebra $\mathfrak{B}$ of a relation algebra $\mathfrak{A}$ to be a regular subalgebra of $\mathfrak{A}$ is that for every subset X

of $\mathfrak{B}$, if $\sum X = 1$ in $\mathfrak{B}$, then $\sum X = 1$ in $\mathfrak{A}$. The necessity of the condition is obvious: it is part of the definition of a regular subalgebra. To prove sufficiency, suppose the condition is satisfied, and let X_0 be an arbitrary subset of $\mathfrak{B}$ that has a supremum r in $\mathfrak{B}$. It is to be proved that r is the supremum of X_0 in $\mathfrak{A}$. Write $X = \{-r\} \cup X_0$ and observe that

$$\{r \cdot s : s \in X\} = X_0,$$

because $r \cdot -r = 0$ and $r \cdot s = s$ for every s in X_0 (since r is an upper bound of X_0). The supremum of X in $\mathfrak{B}$ is 1. Indeed, 1 is obviously an upper bound of X in $\mathfrak{B}$. Suppose now that t is any upper bound of X in $\mathfrak{B}$. In particular, t is an upper bound of X_0, because X_0 is included in X; and therefore $t \geq r$, because r is the least upper bound of X_0 in $\mathfrak{B}$. Also, $t \geq -r$, since $-r$ is in X, so

$$t \geq r + -r = 1.$$

Thus, 1 is the least upper bound of X in $\mathfrak{B}$. The assumed condition now implies that 1 is the supremum of X in $\mathfrak{A}$. Consequently,

$$r = r \cdot 1 = r \cdot \sum X = \sum\{r \cdot s : s \in X\} = \sum X_0$$

in $\mathfrak{A}$.

It is not difficult to check that a subalgebra $\mathfrak{B}$ of a relation algebra $\mathfrak{A}$ is a regular subalgebra just in case every subset of $\mathfrak{B}$ that has an infimum in $\mathfrak{B}$ has the same infimum in $\mathfrak{A}$. This condition is, in turn, equivalent to the condition that for every subset X of $\mathfrak{B}$, if $\prod X = 0$ in $\mathfrak{B}$, then $\prod X = 0$ in $\mathfrak{A}$.

It is not true that the union of a directed system of regular subalgebras of a relation algebra $\mathfrak{A}$ is again a regular subalgebra of $\mathfrak{A}$ (see Lemma 6.7 and the exercises), but there is a version of Lemma 6.13 that holds. Call a system $(\mathfrak{A}_i : i \in I)$ of relation algebras a *directed system of regular subalgebras* if any two algebras $\mathfrak{A}_i$ and $\mathfrak{A}_j$ in the system are always regular subalgebras of some third algebra $\mathfrak{A}_k$ in the system.

Lemma 6.17. *Every algebra in a non-empty, regular directed system of relation algebras is a regular subalgebra of the union algebra.*

Proof. Consider a regular directed system of relation algebras

$$(\mathfrak{A}_i : i \in I), \tag{1}$$

and write $\mathfrak{A}$ for the union of the system. Observe that $\mathfrak{A}$ is a relation algebra, and (1) is a directed system of subalgebras of $\mathfrak{A}$, by Lemma 6.13.

To prove that each algebra $\mathfrak{A}_i$ is a regular subalgebra of $\mathfrak{A}$, let X be a subset of $\mathfrak{A}_i$, and r an element in $\mathfrak{A}_i$ such that r is the supremum of X in $\mathfrak{A}_i$. Certainly, r is an upper bound of X in $\mathfrak{A}$. To see that it is the least upper bound, consider an arbitrary upper bound t of X in $\mathfrak{A}$. Since $\mathfrak{A}$ is the union of the system in (1), there must be an algebra $\mathfrak{A}_j$ in the system that contains t. The system is assumed to be regularly directed, so there is an algebra $\mathfrak{A}_k$ in the system such that $\mathfrak{A}_i$ and $\mathfrak{A}_j$ are both regular subalgebras of $\mathfrak{A}_k$. In particular, r is the supremum of the set X in $\mathfrak{A}_k$, and the element t belongs to $\mathfrak{A}_k$. As t is assumed to be an upper bound, and r the supremum, of X, we must have $r \le t$ in $\mathfrak{A}_k$, and therefore also in $\mathfrak{A}$. It follows that r is the least upper bound of X in $\mathfrak{A}$. □

A subalgebra of an atomic relation algebra need not be atomic. Regular subalgebras have the rather curious property that they do preserve the attribute of being atomic.

Theorem 6.18. *A regular subalgebra of an atomic relation algebra is atomic.*

Proof. Let $\mathfrak{A}$ be an atomic relation algebra, and $\mathfrak{B}$ a regular subalgebra of $\mathfrak{A}$. It is to be shown that every non-zero element in $\mathfrak{B}$ is above an atom in $\mathfrak{B}$. Fix a non-zero element r in $\mathfrak{B}$, and choose an atom s in $\mathfrak{A}$ that is below r. Such an atom certainly exists, by the assumption that $\mathfrak{A}$ is atomic. The set X of elements in $\mathfrak{B}$ that are above s (in $\mathfrak{A}$) contains r, by the choice of s. Moreover, for every element t in $\mathfrak{B}$, exactly one of t and $-t$ belongs to X, since s, as an atom, is below exactly one of these two elements. Finally and most importantly, X has a non-zero lower bound in $\mathfrak{B}$. To see this, assume to the contrary that no non-zero lower bound of X exists in $\mathfrak{B}$. Since 0 is clearly a lower bound of X in $\mathfrak{B}$, it follows that 0 must be the greatest lower bound of X in $\mathfrak{B}$. Consequently, 0 is the greatest lower bound of X in $\mathfrak{A}$, by the assumption that $\mathfrak{B}$ is a regular subalgebra of $\mathfrak{A}$. This conclusion contradicts the obvious fact that s is a non-zero lower bound of X in $\mathfrak{A}$.

Let p be a non-zero lower bound of X in $\mathfrak{B}$. For each element t in $\mathfrak{B}$, exactly one of t and $-t$ is in X, and therefore exactly one of these two elements is above p. (If both of them were above p, then p would be

zero.) Consequently, p is an atom in $\mathfrak{B}$. Since p is below every element in X, it must in particular be below r. $\square$

The next lemma characterizes the property of being a regular subalgebra that is atomic.

Lemma 6.19. *The following conditions on a subalgebra $\mathfrak{B}$ of a relation algebra $\mathfrak{A}$ are equivalent.*

(i) *$\mathfrak{B}$ is a regular subalgebra of $\mathfrak{A}$ that is atomic.*
(ii) *The sum in $\mathfrak{A}$ of the set of atoms in $\mathfrak{B}$ is* 1.
(iii) *Every non-zero element in $\mathfrak{A}$ has a non-zero meet with some atom in $\mathfrak{B}$.*

Proof. Write W for the set of atoms in $\mathfrak{B}$. If condition (i) holds, then $1 = \sum W$ in $\mathfrak{B}$, because $\mathfrak{B}$ is atomic; and therefore $1 = \sum W$ in $\mathfrak{A}$, because $\mathfrak{B}$ is a regular subalgebra of $\mathfrak{A}$. Thus, condition (ii) holds.

Assume now that condition (ii) holds, with goal of deriving condition (i). Condition (ii) implies, in particular, that $1 = \sum W$ in $\mathfrak{B}$, since this equation is assumed to hold in $\mathfrak{A}$, and since all of the elements involved in this equation belong to $\mathfrak{B}$. Consequently, $\mathfrak{B}$ must be atomic. In more detail, if s is any non-zero element in $\mathfrak{B}$, then

$$s = s \cdot 1 = s \cdot \sum W = \sum\{s \cdot r : r \in W\} \tag{1}$$

in $\mathfrak{B}$, so $s \cdot r \neq 0$ for some atom r in $\mathfrak{B}$, and for that atom r we obviously have $r \leq s$.

In order to show that $\mathfrak{B}$ is a regular subalgebra of $\mathfrak{A}$, consider any subset X of $\mathfrak{B}$ such that the equation $\sum X = 1$ holds in $\mathfrak{B}$. It must be shown that this equation also holds in $\mathfrak{A}$, by the remarks preceding Theorem 6.18. Let t be any upper bound of X in $\mathfrak{A}$. For each element r in W, we have $r \leq 1 = \sum X$ in $\mathfrak{B}$, and therefore $r \leq s$ for some s in X, because r is an atom, and X a set of elements, in $\mathfrak{B}$. Of course, $s \leq t$, since t is assumed to be an upper bound of X in $\mathfrak{A}$, so $r \leq t$. This argument shows that t is above each element in W. Since 1 is assumed to be the least upper bound of the set W in $\mathfrak{A}$, by condition (ii), it follows that $t = 1$. Conclusion: 1 is the unique upper bound, and therefore the least upper bound, of the set X in $\mathfrak{A}$.

Turn now to the proof of the equivalence of conditions (ii) and (iii). If condition (ii) holds, and if s is any non-zero element in $\mathfrak{A}$, then the argument in (1) shows that $s \cdot r \neq 0$ for some element r in W, so condition (iii) holds. On the other hand, if condition (iii) holds, and

if s is any element in $\mathfrak{A}$ that is different from 1, then $-s$ is a non-zero element in $\mathfrak{A}$, so there must be an element r in W such that $-s \cdot r \neq 0$. It follows that s cannot be an upper bound of the set W in $\mathfrak{A}$, so 1 is the unique upper bound, and therefore the least upper bound, of W in $\mathfrak{A}$. □

Corollary 6.20. *A necessary and sufficient condition for a subalgebra $\mathfrak{B}$ of an atomic relation algebra $\mathfrak{A}$ to be a regular subalgebra is that 1 be the supremum in $\mathfrak{A}$ of the set of atoms in $\mathfrak{B}$.*

Proof. If $\mathfrak{B}$ is a regular subalgebra of $\mathfrak{A}$, then $\mathfrak{B}$ is atomic, by Theorem 6.18, and therefore 1 is the supremum in $\mathfrak{A}$ of the set of atoms in $\mathfrak{B}$, by Lemma 6.19. On the other hand, if 1 is the supremum in $\mathfrak{A}$ of the set of atoms in $\mathfrak{B}$, then $\mathfrak{B}$ is a regular subalgebra of $\mathfrak{A}$, by Lemma 6.19. □

The proofs of the preceding theorem, lemma, and corollary make no mention of the extra-Boolean operations of the algebras involved. Consequently, the results are actually valid in the general context of Boolean algebras with arbitrary extra-Boolean operations. We shall make use of this fact in the next section.

6.6 Atomic subalgebras

The next theorem presents a method for constructing atomic subalgebras of any relation algebra, and indeed of any Boolean algebra with completely distributive operators, even an atomless one.

Theorem 6.21. *Suppose $\mathfrak{A}$ is a Boolean algebra with complete operators, and W is a subset of $\mathfrak{A}$ with the following properties.*

(i) *The elements in W are disjoint and sum to* 1*.*
(ii) *The element* 1’ *is a sum of elements in W.*
(iii) *If p is in W, then $p^{\smile}$ is a sum of elements in W.*
(iv) *If p and q are in W, then $p\,;q$ is a sum of elements in W.*

The set of sums $\sum X$ such that X is a subset W and $\sum X$ exists in $\mathfrak{A}$ is then the universe of a regular subalgebra of $\mathfrak{A}$ that is atomic, and the atoms of this subalgebra are just the non-zero elements in W. If, in addition, $\mathfrak{A}$ is complete, then the subalgebra is a complete subalgebra of $\mathfrak{A}$.

Proof. We begin with a preliminary remark. If an element r in $\mathfrak{A}$ is the sum of a subset X of W, then X must contain all of the non-zero elements in W that are below r, and $-r$ must be the sum of the elements in the set $W \sim X$. The set X may also contain 0, provided that 0 is in W. For the proof, observe that every element in X is obviously below r, since r is assumed to be the supremum of X. If t is an element in W that is not in X, then t must be disjoint from every element in X, by the first part of condition (i), and therefore

$$t \cdot r = t \cdot (\sum X) = \sum\{t \cdot s : s \in X\} = 0,$$

by Boolean algebra. It follows that t cannot be below r unless t is 0. Thus, every non-zero element in W that is below r must belong to X. This argument also shows that every element in $W \sim X$ is below $-r$. Since $\sum W = 1$, by the second part of condition (i), we may conclude that

$$\begin{aligned} -r = -r \cdot 1 = -r \cdot (\textstyle\sum W) &= \textstyle\sum\{-r \cdot t : t \in W\} \\ &= \textstyle\sum\{-r \cdot t : t \in W \sim X\} = \textstyle\sum\{t : t \in W \sim X\}, \end{aligned}$$

by the preceding observations and Boolean algebra.

Let B be the set of sums defined in the conclusion of the theorem. Condition (ii) implies that B contains 1'. To show that B is closed under the operations of $\mathfrak{A}$, consider elements r and s in B, say

$$r = \sum X \qquad \text{and} \qquad s = \sum Y,$$

where X and Y are subsets of W. Write

$$\begin{aligned} X \diamond Y &= \{t \in W : t \leq p \mathbin{;} q \text{ for some } p \in X \text{ and } q \in Y\}, \\ X^* &= \{t \in W : t \leq p^{\smile} \text{ for some } p \in X\}. \end{aligned}$$

It is not difficult to see that

$$r + s = \sum Z, \quad \text{where } Z = X \cup Y, \tag{1}$$
$$-r = \sum Z, \quad \text{where } Z = W \sim X, \tag{2}$$
$$r \mathbin{;} s = \sum Z, \quad \text{where } Z = X \diamond Y, \tag{3}$$
$$r^{\smile} = \sum Z, \quad \text{where } Z = X^*. \tag{4}$$

These equations and condition (ii) imply that B contains the distinguished constant 1' and is closed under the operations of $\mathfrak{A}$, so B is a subuniverse of $\mathfrak{A}$.

Equation (2) follows directly from the preliminary observation made in the first paragraph. We focus on the proof of (3), and leave the proofs of (1) and (4) as an exercise. For the elements r and s defined above, we have

$$\begin{aligned} r \,;\, s &= (\textstyle\sum X) \,;\, (\textstyle\sum Y) \\ &= \textstyle\sum\{p \,;\, q : p \in X \text{ and } q \in Y\} \\ &= \textstyle\sum\{\textstyle\sum\{t \in W : t \leq p \,;\, q\} : p \in X \text{ and } q \in Y\} \\ &= \textstyle\sum(X \diamond Y). \end{aligned}$$

The first equality uses the assumptions on r and s, and the second uses the assumed complete distributivity of the operation $;$. The third equality follows from condition (iv) and the preliminary remark of the first paragraph, which together imply that for p and q in W, the element $p \,;\, q$ must be the sum of all of the elements in W that are below $p \,;\, q$. The fifth equality uses the definition of the set $X \diamond Y$ and the general associative law for addition.

The preceding argument shows that the set B is the universe of a subalgebra $\mathfrak{B}$ of $\mathfrak{A}$. Every element in $\mathfrak{B}$ is, by definition, a sum of elements in W, so the non-zero elements in W are clearly the minimal elements in $\mathfrak{B}$, that is to say, they are atoms. The unit in $\mathfrak{A}$ is the sum of the set of all elements in W, by condition (i), so it is obviously the sum of the set of all non-zero elements in W, that is to say, it is the sum of the set of atoms in $\mathfrak{B}$. Apply Lemma 6.19 to conclude that $\mathfrak{B}$ is a regular subalgebra of $\mathfrak{A}$ that is atomic.

Finally, if $\mathfrak{A}$ is complete, then the supremum of every subset of W exists in $\mathfrak{A}$, and therefore belongs to $\mathfrak{B}$, by the definition of $\mathfrak{B}$. Consider now an arbitrary subset X of $\mathfrak{B}$. Since $\mathfrak{A}$ is complete, the set X has a supremum in $\mathfrak{A}$, say t. For each element r in X, there is a subset W_r of W such that $r = \sum W_r$ in $\mathfrak{A}$, by the definition of $\mathfrak{B}$. Write

$$Y = \bigcup\{W_r : r \in X\},$$

and observe that Y is a subset of W. The definition of t and the general associative law for addition in $\mathfrak{A}$ imply that

$$t = \textstyle\sum\{r : r \in X\} = \textstyle\sum\{\textstyle\sum W_r : r \in X\} = \textstyle\sum Y$$

in $\mathfrak{A}$, so t belongs to $\mathfrak{B}$, by the definition of $\mathfrak{B}$. Thus, $\mathfrak{B}$ is a complete subalgebra of $\mathfrak{A}$. □

We shall refer to the preceding theorem as the *Atomic Subalgebra Theorem*. Warning: the subalgebra $\mathfrak{B}$ defined in the proof is not necessarily generated by W unless W is finite. We shall have a bit more to say about this in the next section. It is natural to ask why we don't require that the elements in the set W be non-zero. The reason is that the elements in W may be specified in a way that renders it inconvenient to say whether any given one of them is, or is not, non-zero. We shall see an example of this in the next section. A version of Theorem 6.21 that applies to Boolean algebras with quasi-complete operators is given in the exercises.

In a relation algebra, the converse of an atom is always an atom, by Lemma 4.1(vii). Consequently, when applied to relation algebras, the preceding theorem has the following somewhat stronger form.

Corollary 6.22. *If the algebra* $\mathfrak{A}$ *in the preceding theorem is a relation algebra*, *then condition* (iii) *may be replaced by the condition that* $p^{\smile}$ *is in* W *whenever* p *is in* W.

We give two applications of the preceding theorem. For the first, let G be any group, and H any subgroup of G. The set W whose elements are the set $G \sim H$ and the (singletons of) elements in H satisfies the conditions of Theorem 6.21 in the group complex algebra $\mathfrak{Cm}(G)$. Indeed, condition (i) is obviously satisfied, and condition (ii) holds because the identity element belongs to H, and therefore also to W. The converse of an element in H is again an element in H, since H is a subgroup and therefore closed under formation of inverses. Consequently, the converse of the set $G \sim H$—that is to say, the set of group inverses of the elements in $G \sim H$—must be $G \sim H$. It follows that the converse of every element in W is again an element in W, so condition (iii) is satisfied. The verification of condition (iv) splits into four cases. Consider elements p and q in W. If p and q are both elements in H, then the product $p\,;q$ is in H, and therefore also in W, since H is a subgroup of G. For the remaining cases, observe that, as a subgroup, H contains the identity element of the group and is closed under the formation of group compositions and inverses:

$$H^{-1} \subseteq H \qquad \text{and} \qquad H \circ H \subseteq H,$$

where the operations on the left sides of these two inclusions are the complex operations of $\mathfrak{Cm}(G)$. It follows that H is a reflexive equivalence element in $\mathfrak{Cm}(G)$ (see Section 5.3). If p is in H and if q is equal to $G \sim H$, then

$$p\,;q = p\,;(G \sim H) = p \circ (G \sim H) = H \circ (G \sim H) = G \sim H,$$

by the definition of relative multiplication in $\mathfrak{Cm}(G)$, the properties of complex multiplication (the complex product of two cosets is equal to the complex product of any element in the first coset with the second coset), and Lemma 5.24(i). Thus, $p\,;q$ belongs to W in this case. The argument when q is in H and p is equal to $G \sim H$ is similar. Finally, if p and q are both equal to $G \sim H$, then

$$p\,;q = (G \sim H)\,;(G \sim H),$$

and this product is either $\varnothing$, H, or G by Lemma 5.24(ii) and Corollary 4.17. (The fact that $\mathfrak{Cm}(G)$ is simple follows from Corollary 9.10.) In any case, the product $p\,;q$ is a sum of elements in W, so condition (iv) is satisfied. Apply the Atomic Subalgebra Theorem in the form of Corollary 6.22 to conclude that the set of all suprema in $\mathfrak{Cm}(G)$ of subsets of W is the universe of a regular subalgebra of $\mathfrak{Cm}(G)$. We denote this subalgebra by $\mathfrak{Cm}(G, H)$. Its elements are the subsets of H and the subsets of G that include $G \sim H$.

6.7 Minimal subalgebras

For the second application of Theorem 6.21, we describe the elements in the minimal subalgebra of an arbitrary relation algebra $\mathfrak{A}$, and we put a bound on the cardinality of this subalgebra. The key point is the analysis of the product 0' ; 0'. Define five elements in $\mathfrak{A}$ by

$$\begin{aligned}
r_1 &= (0'\,;0') \cdot 0',\\
r_2 &= ([(0'\,;0') \cdot 0']\,;1) \cdot 1' = (r_1\,;1) \cdot 1' = \text{domain } r_1,\\
r_3 &= -(0'\,;0') \cdot 0'\\
r_4 &= ([-(0'\,;0') \cdot 0']\,;1) \cdot 1' = (r_3\,;1) \cdot 1' = \text{domain } r_3,\\
r_5 &= -(0'\,;1) = -(0'\,;0' + 0'\,;1') = -(0'\,;0' + 0') = -(0'\,;0') \cdot 1'.
\end{aligned}$$

The element r_1 is the part of 0';0' that lies below the diversity element, while r_2 is the domain of r_1. The element r_3 is the part of $-(0'\,;0')$ that lies below the diversity element, while r_4 is the domain of r_3. The element r_5 is the part of $-(0'\,;0')$ that lies below the identity element, and of course it coincides with its own domain. We shall prove the following theorem.

Theorem 6.23. *The elements of the minimal subalgebra of a relation algebra are just the distinct sums of the subsets of*

$$W = \{r_1, r_2, r_3, r_4, r_5\}.$$

The minimal subalgebra therefore has at most 2^5 *elements, and its atoms are just the non-zero elements in* W.

Proof. The proof proceeds by showing that the set W satisfies conditions (i)–(iv) of Theorem 6.21. Notice that $r_1 + r_3 = 0'$ and

$$\begin{aligned} r_2 + r_4 = [(r_1 + r_3) ; 1] \cdot 1' = (0' ; 1) \cdot 1' &= (0' ; 0' + 0' ; 1') \cdot 1' \\ &= (0' ; 0' + 0') \cdot 1' = (0' ; 0') \cdot 1'. \end{aligned}$$

These computations lead to three conclusions about the set W. First,

$$r_2 + r_4 + r_5 = 1',$$

so W satisfies condition (ii) of Theorem 6.21. Second, the sum of all the elements in W is 1. Third, the three elements

$$r_1 + r_3, \qquad r_2 + r_4, \qquad r_5$$

are mutually disjoint, so in order to show that all the elements in W are disjoint, it suffices to check that r_1 and r_3, and also r_2 and r_4, are disjoint. The disjointness of the first two elements is obvious, but that of the second two takes a bit of computation. Observe that

$$r_1 ; 0' \leq 0' ; 0', \tag{1}$$

because r_1 is below 0', and consequently

$$r_1 ; 1 = r_1 ; (1' + 0') = r_1 ; 1' + r_1 ; 0' \leq r_1 + 0' ; 0' = 0' ; 0', \tag{2}$$

by the definition of 0' and Boolean algebra, the distributive and identity laws for relative multiplication, (1), and the definition of r_1. From (2) and the definition of r_3 it follows that

$$(r_1 ; 1) \cdot r_3 = 0, \tag{3}$$

and therefore

$$(r_1 ; 1) \cdot (r_3 ; 1) = [(r_1 ; 1) \cdot r_3] ; 1 = 0 ; 1 = 0, \tag{4}$$

by the second equation in Lemma 5.15 (the second modular law for equivalence elements, with 1, r_3, and r_1 in place of r, s, and t respectively), (3), and the first dual of Corollary 4.17. The disjointness of r_2 and r_4 follows at once from (4) and the definitions of these two elements. Conclusion: the set W satisfies condition (i) of Theorem 6.21.

To see that W satisfies condition (iii) of the theorem, observe that each element in W is symmetric. For the three subidentity elements, r_2, r_4, and r_5, this follows from the second equation in Lemma 5.20(i). For r_3, we have

$$\begin{aligned} r_3^{\smile} = [-(0' \,;\, 0') \cdot 0']^{\smile} &= [-(0' \,;\, 0')]^{\smile} \cdot 0'^{\smile} = -[(0' \,;\, 0')^{\smile}] \cdot 0'^{\smile} \\ &= -(0'^{\smile} \,;\, 0'^{\smile}) \cdot 0'^{\smile} = -(0' \,;\, 0') \cdot 0' = r_3, \end{aligned}$$

by the definition of r_3, Lemma 4.1(ii),(v), the second involution law, and Lemma 4.7(vi). The computation for r_1 is similar but easier, and is left to the reader.

$;$	r_1	r_2	r_3	r_4	r_5
r_1	$r_1 + r_2$	r_1	0	0	0
r_2	r_1	r_2	0	0	0
r_3	0	0	r_4	r_3	0
r_4	0	0	r_3	r_4	0
r_5	0	0	0	0	r_5

Table 6.1 Relative multiplication table for elements in W.

The proof that W satisfies condition (iv) of Theorem 6.21 is more involved. The operation of relative multiplication is commutative on elements in W, by the second involution law and the fact that each element in W is symmetric. Consequently, it is only necessary to compute the products $r_i \,;\, r_j$ for $1 \leq i \leq j \leq 5$. The values of these products are summarized in Table 6.1. We shall explain in a later chapter how each of the products may be easily determined, but for now we take a brute force approach. Most of the entries in the table are readily checked using Lemmas 5.20(i), 5.48(ii), and 5.51, or simple arguments similar to the ones given in the proofs of those lemmas. For example, since every element in W is its own converse, the domain of every element in W must equal the range of that element. Consequently, $r_1 \,;\, r_2 = r_1$, by Lemma 5.48(ii). The domains of r_1 and r_3 are disjoint, by (4),

so $r_1 ; r_3 = 0$ by Lemma 5.51. The domain of r_4 is equal to that of r_3, so we also get $r_1 ; r_4 = 0$ by Lemma 5.51. Finally,

$$(r_1 ; 1) \cdot r_5 \leq (0' ; 0') \cdot r_5 = 0, \tag{5}$$

by (2) and the definition of r_5. Since

$$\begin{aligned} r_1 ; r_5 = 0 \qquad &\text{if and only if} \qquad (r_1 ; r_5) \cdot 1 = 0, \\ &\text{if and only if} \qquad (r_1 ; 1) \cdot r_5 = 0, \end{aligned}$$

by Boolean algebra, the De Morgan-Tarski laws, and the symmetry of the element r_1, it follows that $r_1 ; r_5 = 0$.

Three of the values in the table are somewhat more difficult to check, namely the values of the relative products

$$r_1 ; r_1, \qquad r_3 ; r_3, \qquad \text{and} \qquad r_3 ; r_5.$$

To compute the first product, observe that r_1 is below both 0' and 1, and therefore

$$r_1 ; r_1 \leq 0' ; 0' \qquad \text{and} \qquad r_1 ; r_1 \leq r_1 ; 1, \tag{6}$$

by the monotony law for relative multiplication. Consequently,

$$\begin{aligned} r_1 ; r_1 = (r_1 ; r_1) \cdot 1 = (r_1 ; r_1) \cdot (0' + 1') &= (r_1 ; r_1) \cdot 0' + (r_1 ; r_1) \cdot 1' \\ &\leq (0' ; 0') \cdot 0' + (r_1 ; 1) \cdot 1' = r_1 + r_2, \end{aligned}$$

by Boolean algebra and the definition of 0', (6), and the definitions of r_1 and r_2. This proves that the product $r_1 ; r_1$ is below the sum $r_1 + r_2$. On the other hand,

$$\begin{aligned} r_1 = (0' ; 0') \cdot 0' &\leq [(0' ; 0'^{\smile}) \cdot 0'] ; [0' \cdot (0'^{\smile} ; 0')] \\ &= [(0' ; 0') \cdot 0'] ; [0' \cdot (0' ; 0')] = r_1 ; r_1, \end{aligned}$$

by the definition of r_1, Lemma 4.25 (with r, s, and t all replaced by 0'), and Lemma 4.7(vi). Also,

$$r_2 = (r_1 ; 1) \cdot 1' \leq r_1 ; [1 \cdot (r_1^{\smile} ; 1')] = r_1 ; r_1^{\smile} = r_1 ; r_1, \tag{7}$$

by the definition of r_2, Lemma 4.19 (with r_1, 1, and 1' in place of r, s, and t respectively), Boolean algebra, the identity law for relative multiplication, and the symmetry of r_1. Consequently, the sum $r_1 + r_2$ is below the relative product $r_1 ; r_1$. Conclusion: $r_1 ; r_1 = r_1 + r_2$.

Turn now to the second product, $r_3 \,;\, r_3$. An argument parallel to the one given for (7) yields

$$r_4 = (r_3 \,;\, 1) \cdot 1' \leq r_3 \,;\, [1 \cdot (r_3^{\smile} \,;\, 1')] = r_3 \,;\, r_3^{\smile} = r_3 \,;\, r_3. \tag{8}$$

To establish the reverse inequality, observe that r_3 is, by its very definition, below 0', so $r_3 \,;\, 0'$ is below $0' \,;\, 0'$, by the monotony law for relative multiplication. Also, r_3 is below $-(0' \,;\, 0')$, so

$$r_3 \cdot (r_3 \,;\, 0') \leq -(0' \,;\, 0') \cdot (0' \,;\, 0') = 0. \tag{9}$$

Consequently,

$$(r_3 \,;\, r_3) \cdot 0' \leq r_3 \,;\, [r_3 \cdot (r_3^{\smile} \,;\, 0')] = r_3 \,;\, [r_3 \cdot (r_3 \,;\, 0')] \leq r_3 \,;\, 0 = 0,$$

by Lemma 4.19 (with r_3 in place of r and s, and 0' in place of t), the symmetry of r_3, (9), the monotony law for relative multiplication, and Corollary 4.17. It follows that the relative product $r_3 \,;\, r_3$ is below the identity element 1', and it is also below $r_3 \,;\, 1$, by the monotony law for relative multiplication, so

$$r_3 \,;\, r_3 \leq (r_3 \,;\, 1) \cdot 1' = r_4. \tag{10}$$

Combine (10) with (8) to conclude that $r_3 \,;\, r_3 = r_4$.

Turn finally to the computation of $r_3 \,;\, r_5$. Observe first that $r_3 \,;\, 1$ is below $0' \,;\, 1$, because r_3 is below 0', and therefore $r_3 \,;\, 1$ is disjoint from r_5, by the definition of r_5. An argument similar to the one given for (7) now yields

$$\begin{aligned} r_3 \,;\, r_5 = (r_3 \,;\, r_5) \cdot 1 \leq r_3 \,;\, &[(r_5 \cdot (r_3^{\smile} \,;\, 1)] \\ &= r_3 \,;\, [(r_5 \cdot (r_3 \,;\, 1)] = r_3 \,;\, 0 = 0. \end{aligned}$$

Table 6.1 makes clear that condition (iv) of Theorem 6.21 is satisfied. Apply the theorem in the form of Corollary 6.22 to conclude that the set of sums of elements in W is a subuniverse of the given relation algebra. It follows that this subuniverse has cardinality less then or equal to the number of subsets of W, which is 2^5. □

6.8 Elementary subalgebras

Subalgebras of relation algebras preserve the finitary operations of addition and multiplication, complement, relative addition, relative multiplication, and converse of the parent algebra. Complete subalgebras preserve also the infinitary operations of forming suprema and infima. There is another kind of subalgebra that preserves all properties expressible in the first-order language of relation algebras (see Section 2.4). A subalgebra $\mathfrak{B}$ of an algebra $\mathfrak{A}$ is called an *elementary subalgebra* if, for every formula Γ with n free variables in the language of relation algebras, and every sequence r of n elements in $\mathfrak{B}$, the sequence r satisfies the formula Γ in $\mathfrak{B}$ if and only if r satisfies Γ in $\mathfrak{A}$. When Γ is a sentence, this simply means that Γ is true in $\mathfrak{B}$ if and only if Γ is true in $\mathfrak{A}$. If $\mathfrak{B}$ is an elementary subalgebra of $\mathfrak{A}$, then $\mathfrak{A}$ is called an *elementary extension* of $\mathfrak{B}$.

The relation of one algebra being an elementary subalgebra of another is *strongly transitive* in the sense of the following lemma.

Lemma 6.24. *If $\mathfrak{B}$ is an elementary subalgebra of $\mathfrak{A}$, and $\mathfrak{C}$ a subalgebra of $\mathfrak{B}$, then $\mathfrak{C}$ is an elementary subalgebra of $\mathfrak{A}$ if and only if it is an elementary subalgebra of $\mathfrak{B}$.*

Proof. Let Γ be a formula with n free variables in the language of relation algebras, and r a sequence of n elements in $\mathfrak{C}$. Of course r is also a sequence of n elements in $\mathfrak{B}$, since $\mathfrak{C}$ is assumed to be a subalgebra of $\mathfrak{B}$. Moreover, r satisfies Γ in $\mathfrak{A}$ if and only if it satisfies Γ in $\mathfrak{B}$, by the assumption that $\mathfrak{B}$ is an elementary subalgebra of $\mathfrak{A}$. Consequently, the requirement that r satisfy Γ in $\mathfrak{C}$ if and only if it satisfies Γ in $\mathfrak{A}$ is equivalent to the requirement that r satisfy Γ in $\mathfrak{C}$ if and only if it satisfies Γ in $\mathfrak{B}$. The first requirement holds for all formulas Γ and all appropriate sequences r if and only if $\mathfrak{C}$ is an elementary subalgebra of $\mathfrak{A}$, and the second requirement holds for all Γ and all appropriate r if and only if $\mathfrak{C}$ is an elementary subalgebra of $\mathfrak{B}$, by the definition of an elementary subalgebra. Combine these observations to arrive at the conclusion of the lemma. $\square$

The fundamental result concerning the existence of elementary subalgebras and extensions is known as the *Löwenheim-Skolem-Tarski Theorem.* There are two versions of this theorem, the *downward* version and the *upward* version. The downward version, in its application

to relation algebras, says that for every subset X of an infinite relation algebra $\mathfrak{A}$, and for every infinite cardinal number κ between the cardinality of X and the cardinality of $\mathfrak{A}$, there is an elementary subalgebra of $\mathfrak{A}$ that includes X as a subset of its universe and has cardinality κ. The upward version says that if a relation algebra $\mathfrak{A}$ has infinite cardinality κ, then for every infinite cardinal $\lambda \geq \kappa$ there is an elementary extension of $\mathfrak{A}$ of cardinality λ. The proofs of these theorems are of course metamathematical in nature. We begin with a lemma which refers to formulas $\Gamma(v_0, v_1, \dots, v_n)$ in the language of relation algebras. The notation is meant to indicate that the free variables occurring in Γ are among the distinct variables $v_0, v_1, \dots, v_n$.

Lemma 6.25. *For $\mathfrak{B}$ to be an elementary subalgebra of a relation algebra $\mathfrak{A}$, it is necessary and sufficient that $\mathfrak{B}$ be a subalgebra of $\mathfrak{A}$ and that $\mathfrak{B}$ satisfy the following condition: for every first-order formula $\Delta(v_0, v_1, \dots, v_n)$ and every sequence $(r_1, \dots, r_n)$ of elements from $\mathfrak{B}$, if the sequence $(r_1, \dots, r_n)$ satisfies the formula $\exists v_0 \Delta$ in $\mathfrak{A}$, then there is an element r_0 in $\mathfrak{B}$ such that the sequence $(r_0, r_1, \dots, r_n)$ satisfies the formula Δ in $\mathfrak{A}$.*

Proof. If $\mathfrak{B}$ is an elementary subalgebra of $\mathfrak{A}$, then obviously $\mathfrak{B}$ satisfies the condition of the lemma. To establish the reverse implication, assume that $\mathfrak{B}$ satisfies the condition of the lemma, and write $\mathcal{S}$ for the set of formulas Γ with the property that any given sequence of elements in $\mathfrak{B}$ satisfies Γ in $\mathfrak{B}$ if and only if the sequence satisfies Γ in $\mathfrak{A}$. It is to be shown that every formula in the language of relation algebras belongs to $\mathcal{S}$. The proof proceeds by induction on formulas.

If Γ is an equation, then a sequence of elements in $\mathfrak{B}$ satisfies Γ in $\mathfrak{B}$ if and only if it satisfies Γ in $\mathfrak{A}$, by Lemma 6.2, because $\mathfrak{B}$ is assumed to be a subalgebra of $\mathfrak{A}$. Thus, the set $\mathcal{S}$ contains all equations. The proof that $\mathcal{S}$ is closed under the formation of negations and implications is straightforward, and proceeds just as in the proof of Lemma 6.2. The details are left to the reader.

The closure of $\mathcal{S}$ under negation implies that $\mathcal{S}$ is closed under universal quantification if and only if it is closed under existential quantification. To show closure under existential quantification, let $\Delta(v_0, v_1, \dots, v_n)$ be any formula in $\mathcal{S}$, and suppose Γ is the formula $\exists v_0 \Delta$. Consider any sequence $(r_1, \dots, r_n)$ of n elements in $\mathfrak{B}$. If $(r_1, \dots, r_n)$ satisfies Γ in $\mathfrak{B}$, then there must be an element r_0 in $\mathfrak{B}$ such that the sequence $(r_0, r_1, \dots, r_n)$ satisfies Δ in $\mathfrak{B}$, by the definition of satisfaction. Since Δ belongs to $\mathcal{S}$, it follows that

the sequence $(r_0, r_1, \ldots, r_n)$ satisfies Δ in $\mathfrak{A}$, by the definition of $\mathcal{S}$, so $(r_1, \ldots, r_n)$ satisfies Γ in $\mathfrak{A}$, again by the definition of satisfaction. On the other hand, if $(r_1, \ldots, r_n)$ satisfies Γ in $\mathfrak{A}$, then the condition of the lemma implies the existence of an element r_0 in $\mathfrak{B}$ such that the sequence $(r_0, r_1, \ldots, r_n)$ satisfies Δ in $\mathfrak{A}$. Since Δ belongs to $\mathcal{S}$, the sequence $(r_0, r_1, \ldots, r_n)$ must also satisfy Δ in $\mathfrak{B}$, by the definition of $\mathcal{S}$, so $(r_1, \ldots, r_n)$ satisfies Γ in $\mathfrak{B}$, by the definition of satisfaction. Thus, Γ belongs to $\mathcal{S}$. Use the principle of induction on formulas to conclude that all formulas in the language of relation algebras belong to $\mathcal{S}$. $\square$

Here is the downward Löwenheim-Skolem-Tarski Theorem.

Theorem 6.26. *Let κ be any infinite cardinal. For each relation algebra $\mathfrak{A}$ of cardinality at least κ, and each subset X of $\mathfrak{A}$ of cardinality at most κ, there is an elementary subalgebra of $\mathfrak{A}$ that includes X as a subset and has cardinality κ.*

Proof. By adjoining new elements from $\mathfrak{A}$ to X, if necessary, it may be assumed that X has cardinality κ. Define a sequence of subsets X_i of $\mathfrak{A}$ by induction on natural numbers i. The set X_0 is defined to be X. Assume now that X_i has been defined, and define the set X_{i+1} as follows. For each formula $\Gamma(v_0, v_1, \ldots, v_n)$ in the first-order language of relation algebras, and each sequence $(r_1, \ldots, r_n)$ of elements from X_i that satisfies the formula $\exists v_0 \Gamma$ in $\mathfrak{A}$, choose an element r_0 in $\mathfrak{A}$ such that the sequence $(r_0, r_1, \ldots, r_n)$ satisfies Γ in $\mathfrak{A}$. This is possible by the definition of satisfaction. Let X_{i+1} be the set consisting of all the elements chosen in this way. Every element in X_i certainly belongs to X_{i+1}. Indeed, if Γ is the formula $v_0 = v_1$, then every element r_1 in X_i satisfies the formula $\exists v_0 \Gamma$ in $\mathfrak{A}$, and the element r_0 chosen for the formula Γ and the sequence (r_1) must of course be r_1; consequently, r_1 belongs to X_{i+1}. Thus,

$$X_0 \subseteq X_1 \subseteq \ldots \subseteq X_i \subseteq \ldots . \tag{1}$$

An easy argument by induction on i, using the assumption that the set X has cardinality κ, and the fact that the language of relation algebras is countable, shows that each set X_i has cardinality κ for each natural number i. Let B be the union of the sets X_i, and observe that B includes X, by the definition of X_0. Also, B has cardinality κ, because the union of a countably infinite sequence of sets of infinite cardinality κ must have cardinality κ.

It requires a bit more work to see that B is a subuniverse of $\mathfrak{A}$. Suppose, for example, that r_1 and r_2 are elements in B. These two elements must belong to the set X_i for some natural number i, by (1) and the definition of B. Take Γ to be the equation $v_0 = v_1 ; v_2$, and observe that the formula $\exists v_0 \Gamma$ is satisfied by the sequence (r_1, r_2) in $\mathfrak{A}$. Consequently, there must be an element r_0 in X_{i+1} such that (r_0, r_1, r_2) satisfies the equation Γ in $\mathfrak{A}$, by the definition of the set X_{i+1}. Since the relative product $r_1 ; r_2$ coincides with r_0, by the definition of Γ, it follows that this relative product belongs to the set X_{i+1} and therefore also to the union set B. Thus, B is closed under relative multiplication. Similar arguments show that B contains 1' and is closed under the remaining operations of $\mathfrak{A}$, so B is a subuniverse of $\mathfrak{A}$.

Let $\mathfrak{B}$ be the subalgebra of $\mathfrak{A}$ with universe B. To prove that $\mathfrak{B}$ is in fact an elementary subalgebra of $\mathfrak{A}$, it suffices to show that $\mathfrak{B}$ satisfies the condition of Lemma 6.25. Consider a formula $\Gamma(v_0, v_1, \dots, v_n)$, and suppose $(r_1, \dots, r_n)$ is a sequence of elements in $\mathfrak{B}$ that satisfies the formula $\exists v_0 \Gamma$ in $\mathfrak{A}$. There must be a natural number i such that the set X_i contains each of the elements in this sequence, by (1). Consequently, there is an element r_0 in X_{i+1} such that the sequence $(r_0, r_1, \dots, r_n)$ satisfies the formula Γ in $\mathfrak{A}$, by the definition of the set X_{i+1}. The element r_0 clearly belongs to $\mathfrak{B}$, by the definition of $\mathfrak{B}$. Thus, the condition in Lemma 6.25 does hold for $\mathfrak{B}$, so $\mathfrak{B}$ is an elementary subalgebra of $\mathfrak{A}$, by the lemma. □

Notice the similarity in the general form of the proofs of Lemma 6.5 and Theorem 6.26. In both proofs, an increasing sequence of sets X_i is constructed whose union is the desired subalgebra. At the ith step of the construction, new elements are adjoined to the set X_i to obtain a set X_{i+1} that is the closure of X_i under single applications of certain operations. In the case of Lemma 6.5, the operations are those of the algebra $\mathfrak{A}$ while in the case of Theorem 6.26, they are the operations induced in $\mathfrak{A}$ by existential quantifications. These latter operations are sometimes called *Skolem functions*.

The following corollary is an immediate consequence of Theorem 6.26.

Corollary 6.27. *For every countable subset X of a relation algebra $\mathfrak{A}$, there is a countable elementary subalgebra of $\mathfrak{A}$ that includes X as a subset.*

Turn now to the upward Löwenheim-Skolem-Tarski Theorem.

Theorem 6.28. *A relation algebra of infinite cardinality κ has an elementary extension of cardinality λ for every cardinal $\lambda \geq \kappa$.*

Proof. Let $\mathfrak{A}$ be a relation algebra of infinite cardinality κ. Adjoin to the language $\mathcal{L}$ of relation algebras two systems of new individual constant symbols, all distinct from one another: first, adjoin an individual constant symbol $\boldsymbol{r}$ for each element r in $\mathfrak{A}$; and second, adjoin also a system $(\boldsymbol{s}_i : i \in I)$ of λ individual constant symbols. Let $\mathcal{S}$ be the set of sentences obtained in the following way: whenever $\Gamma(v_0, \dots, v_{n-1})$ is a formula in $\mathcal{L}$ and $(r_0, \dots, r_{n-1})$ a sequence of elements in $\mathfrak{A}$ that satisfies Γ in $\mathfrak{A}$, put into $\mathcal{S}$ the sentence

$$\Gamma(\boldsymbol{r}_0, \dots, \boldsymbol{r}_n)$$

obtained from Γ by replacing the free occurrences of each of the variables $v_0, \dots, v_{n-1}$ with the individual constant symbols $\boldsymbol{r}_0, \dots, \boldsymbol{r}_{n-1}$ respectively. (The set $\mathcal{S}$ is sometimes called the *elementary diagram* of $\mathfrak{A}$.) Let $\mathcal{T}$ be the set of sentences of the form $\boldsymbol{s}_i \neq \boldsymbol{s}_j$ for distinct indices i and j in I.

Every finite subset of the set of sentences $\mathcal{S} \cup \mathcal{T}$ has a model that is obtained from $\mathfrak{A}$ by adding elements of $\mathfrak{A}$ as distinguished constants interpreting the new individual constants occurring in the finite subset. (The assumption that $\mathfrak{A}$ is infinite is needed to ensure that we can always adjoin distinguished constants to $\mathfrak{A}$ that make the sentences in any given finite subset of $\mathcal{T}$ true.) Apply the Compactness Theorem (see Section 2.4) to conclude that the set $\mathcal{S} \cup \mathcal{T}$ has a model $\mathfrak{B}^*$. The algebra $\mathfrak{B}$ obtained from $\mathfrak{B}^*$ by deleting the interpretations of the new individual constant symbols as distinguished constants (but still keeping these elements in the algebra) is a relation algebra that contains a copy of $\mathfrak{A}$ as an elementary subalgebra, because $\mathfrak{B}^*$ is a model of $\mathcal{S}$; and $\mathfrak{B}$ has cardinality at least λ, because $\mathfrak{B}^*$ is a model of $\mathcal{T}$.

The Exchange Principle (see Section 7.7) implies that the copy of $\mathfrak{A}$ inside $\mathfrak{B}$ may be exchanged for $\mathfrak{A}$ itself; consequently, without loss of generality it may be assumed that $\mathfrak{A}$ itself is an elementary subalgebra of $\mathfrak{B}$. Since $\mathfrak{B}$ has cardinality at least λ, and $\mathfrak{A}$ has cardinality $\kappa \leq \lambda$, an application of the downward Löwenheim-Skolem-Tarski Theorem yields an elementary subalgebra of $\mathfrak{B}$ of cardinality λ that includes $\mathfrak{A}$ as a subalgebra. Use Lemma 6.24 to conclude that this elementary subalgebra of $\mathfrak{B}$ must be an elementary extension of $\mathfrak{A}$. □

A number of the results concerning directed systems of subalgebras have versions that apply to elementary subalgebras. A system $(\mathfrak{A}_i : i \in I)$ of algebras is said to be a *directed system of elementary subalgebras* if any two members $\mathfrak{A}_i$ and $\mathfrak{A}_j$ in the system are always elementary subalgebras of some third member $\mathfrak{A}_k$. The next lemma is the analogue of Lemma 6.7

Lemma 6.29. *The union of a non-empty, directed system of elementary subalgebras of a relation algebra* $\mathfrak{A}$ *is again an elementary subalgebra of* $\mathfrak{A}$.

Proof. Consider a directed system

$$(\mathfrak{B}_i : i \in I) \tag{1}$$

of elementary subalgebras of $\mathfrak{A}$, and let $\mathfrak{B}$ be the union of this system. Certainly, $\mathfrak{B}$ is a subalgebra of $\mathfrak{A}$, by Lemma 6.7. It is to be shown that $\mathfrak{B}$ is in fact an elementary subalgebra of $\mathfrak{A}$. To this end, let

$$\Gamma(v_0, \ldots, v_n)$$

be a first-order formula in the language of relation algebras, and

$$(r_1, \ldots, r_n) \tag{2}$$

a sequence of elements in $\mathfrak{B}$ that satisfies the formula $\exists v_0 \Gamma$ in $\mathfrak{A}$. Each of the elements in (2) belongs to one of the algebras in the system (1), by the definition of $\mathfrak{B}$ as the union of this system. Since the system is directed, there must be an algebra $\mathfrak{B}_k$ to which all of the elements in the sequence belong. By assumption, $\mathfrak{B}_k$ is an elementary subalgebra of $\mathfrak{A}$, and the sequence (2) is assumed to satisfy the formula $\exists v_0 \Gamma$ in $\mathfrak{A}$, so (2) must also satisfy this formula in $\mathfrak{B}_k$. Consequently, there must be an element r_0 in $\mathfrak{B}_k$ such that the sequence

$$(r_0, r_1, \ldots, r_n) \tag{3}$$

satisfies Γ in $\mathfrak{B}_k$, by the definition of satisfaction. Use again the assumption that $\mathfrak{B}_k$ is an elementary subalgebra of $\mathfrak{A}$ to see that the sequence (3) satisfies Γ in $\mathfrak{A}$. Of course, r_0 also belongs to the union algebra $\mathfrak{B}$. Apply Lemma 6.25 to conclude that $\mathfrak{B}$ is an elementary subalgebra of $\mathfrak{A}$. □

An immediate consequence of Lemma 6.29 is the following analogue of Corollary 6.8.

Corollary 6.30. *The union of a non-empty chain of elementary subalgebras of a relation algebra $\mathfrak{A}$ is again an elementary subalgebra of $\mathfrak{A}$.*

The next lemma gives an elementary analogue of Corollary 6.10.

Lemma 6.31. *Every relation algebra is the directed union of a system of countable elementary subalgebras.*

Proof. Consider the system

$$(\mathfrak{A}_i : i \in I) \tag{1}$$

of all countable elementary subalgebras of $\mathfrak{A}$. If $\mathfrak{A}_i$ and $\mathfrak{A}_j$ are any two algebras in (1), then the union of the universes of $\mathfrak{A}_i$ and $\mathfrak{A}_j$ is a countable subset of $\mathfrak{A}$, so there must be a countable elementary subalgebra of $\mathfrak{A}$ that includes this union as a subset, by Corollary 6.27. That subalgebra must occur as one of the elementary subalgebras $\mathfrak{A}_k$ in (1), by the very definition of system (1). Both $\mathfrak{A}_i$ and $\mathfrak{A}_j$ are subalgebras (and in fact elementary subalgebras) of $\mathfrak{A}_k$, since all three are elementary subalgebras of $\mathfrak{A}$ (see Lemma 6.24). Thus, system (1) is directed.

The singleton of each element r in $\mathfrak{A}$ is a countable subset of $\mathfrak{A}$, so there must be a countable elementary subalgebra of $\mathfrak{A}$ that contains r as an element, again by Corollary 6.27. Consequently, every element in $\mathfrak{A}$ belongs to one of the algebras in (1), so $\mathfrak{A}$ must be the union of the algebras in (1). □

The next lemma is the analogue of Lemma 6.13.

Lemma 6.32. *The union of a non-empty, elementary directed system of relation algebras is a relation algebra that is an elementary extension of every algebra in the system.*

Proof. Consider a non-empty, elementary directed system of relation algebras

$$(\mathfrak{A}_i : i \in I), \tag{1}$$

and write $\mathfrak{A}$ for the union of this system. It follows from Lemma 6.7 that $\mathfrak{A}$ is a relation algebra extending each algebra in the system. It remains to prove that $\mathfrak{A}$ is in fact an elementary extension of each algebra in the system. To this end, write $\mathcal{S}$ for the set of formulas Γ with the property that for all indices i, and all appropriate sequences r of elements in $\mathfrak{A}_i$, the formula Γ is satisfied by r in $\mathfrak{A}_i$ if and only if it is

satisfied by r in $\mathfrak{A}$. It is to be shown that every formula in the language of relation algebras belongs to $\mathcal{S}$. The proof proceeds by induction on formulas.

The set $\mathcal{S}$ contains all equations, by Lemma 6.2. The argument that $\mathcal{S}$ is closed under the formation of negations and implications is the same as in the proof of Lemma 6.2, and is left to the reader. The closure of $\mathcal{S}$ under negation implies that $\mathcal{S}$ is closed under universal quantification if and only if it is closed under existential quantification, so it suffices to treat the case of an existential quantifier. For notational simplicity, assume that $\Gamma(v_1, \cdots, v_n)$ has the form $\exists v_0 \Delta$, where $\Delta(v_0, \ldots, v_n)$ is a formula in $\mathcal{S}$.

Fix an index i in I, and consider a sequence

$$r = (r_1, \ldots, r_n)$$

of elements in $\mathfrak{A}_i$. If r satisfies Γ in $\mathfrak{A}_i$, then there is a sequence

$$s = (s_0, \ldots, s_n) \tag{2}$$

of elements in $\mathfrak{A}_i$, with $s_\ell = r_\ell$ for $\ell = 1, \ldots, n$, such that s satisfies Δ in $\mathfrak{A}_i$, by the definition of satisfaction. The assumption that Δ belongs to $\mathcal{S}$, and the definition of the set $\mathcal{S}$, imply that s satisfies Δ in $\mathfrak{A}$, so r must also satisfy Γ in $\mathfrak{A}$, by the definition of satisfaction.

To establish the reverse implication, assume r satisfies Γ in $\mathfrak{A}$. There must be a sequence (2) of elements in $\mathfrak{A}$, with $s_\ell = r_\ell$ for $\ell = 1, \ldots, n$, such that s satisfies Δ in $\mathfrak{A}$, by the definition of satisfaction. Notice that s_ℓ belongs to $\mathfrak{A}_i$ for $\ell = 1, \ldots, n$, because it coincides with r_ℓ. The algebra $\mathfrak{A}$ is the union of system (1), so there must be an algebra $\mathfrak{A}_j$ in the system that contains the element s_0. The system is assumed to be elementary directed, so there must be an algebra $\mathfrak{A}_k$ in the system that is an elementary extension of both $\mathfrak{A}_i$ and $\mathfrak{A}_j$. In particular, the elements in the sequence s all belong to $\mathfrak{A}_k$. Since s satisfies the formula Δ in $\mathfrak{A}$, and since Δ is assumed to belong to the set $\mathcal{S}$, it follows from the definition of $\mathcal{S}$ that s must satisfy Δ in $\mathfrak{A}_k$. The definition of satisfaction therefore implies that r satisfies Γ in $\mathfrak{A}_k$. Since $\mathfrak{A}_i$ is an elementary subalgebra of $\mathfrak{A}_k$, and the elements in r all belong to $\mathfrak{A}_i$, it may be concluded that r satisfies Γ in $\mathfrak{A}_i$, as desired. The observations of the last two paragraphs show that the formula Γ belongs to $\mathcal{S}$. Use the principle of induction on formulas to conclude that all formulas in the language of relation algebras belong to $\mathcal{S}$. $\square$

A special case of the preceding lemma occurs when the directed system is in fact a chain in the sense that it is linearly ordered by the relation of being an elementary subalgebra.

Corollary 6.33. *The union of a non-empty elementary chain of relation algebras is a relation algebra that is an elementary extension of every algebra in the chain.*

6.9 Historical remarks

The notions of a subalgebra and the subalgebra generated by a set are general algebraic in nature and apply to arbitrary algebras. In particular, all of the notions and results in Sections 6.1–6.4 are special cases of general results about arbitrary algebras. Good sources for this information are [20], [39], and [84]. The specific example given in Section 6.3 of an infinite set relation algebra with a single generator is due to Tarski [112].

The notions of a regular subalgebra and a complete subalgebra come from the theory of Boolean algebras, and the results in Section 6.5 apply to arbitrary Boolean algebras, and therefore to arbitrary Boolean algebras with additional operations (possibly non-distributive). Lemma 6.17 and the example implicit in Exercise 6.25 (see the selected "Hints and Solutions" to the exercises), which shows that the union of a directed system of regular subalgebras need not be a regular subalgebra, are due to Givant. Theorem 6.18 (for arbitrary Boolean algebras with or without additional operations) is due to Robin Hirsch and Ian Hodkinson [43] (see also Lemma 2.16 in [44]). Earlier, Alexander Abian [1] proved that if a monomorphism from a Boolean ring $\mathfrak{B}$ into a Boolean ring of all subsets of some set preserves all existing suprema, then $\mathfrak{B}$ must be atomic. This paper remained largely unknown, and was unknown to Hirsch and Hodkinson at the time that they discovered their theorem. The equivalence of conditions (i) and (iii) in Lemma 6.19 is essentially due to Hirsch and Hodkinson, although their formulation is slightly weaker than ours; see Lemma 2.17 in [44]. The equivalence of conditions (i) and (ii) in Lemma 6.19, and Corollary 6.20, are due to Givant.

A version of Theorem 6.21 is valid for Boolean algebras with completely distributive operators of an arbitrary similarity type. The conditions in (iii) and (iv) of the theorem must be replaced by a condition

that applies to completely distributive operators of arbitrary rank n, and not just of ranks 1 and 2. The general theorem is an unpublished result of Givant and Tarski. An extension of this result to Boolean algebras with quasi-complete operators (see Exercises 6.34 and 6.35) is due to Givant. The application of Theorem 6.21 to the analysis of the subalgebra $\mathfrak{Cm}(G, H)$ of a group complex algebra $\mathfrak{Cm}(G)$ is also due to Givant. The ideas underlying the analysis of minimal relation algebras go back to results in Jónsson-Tarski [55] (see, in particular, their Theorems 4.33, 4.35, and 4.36). The use of these ideas to prove Theorem 6.23 is due to Tarski. The particular proof presented in Section 6.6 is due to Givant. The elegant derivations of the equations

$$r_1 \mathbin{;} r_1 = r_1 + r_2, \qquad r_3 \mathbin{;} r_3 = r_4, \qquad r_3 \mathbin{;} r_5 = 0$$

that are given in the proof of Theorem 6.23 are due to Maddux. Theorem 6.23 is closely related to the well-known theorem that the first-order theory of equality admits elimination of quantifiers. In fact, Theorem 6.23 can be viewed as a version of the quantifier elimination theorem for the theory of equality when this theory is formalized within the framework of a logic with just three variables.

The notions and results in Section 6.8 are valid for arbitrary relational structures, subject to some restrictions on the number of fundamental operations and relations. The original result in this domain is due to Leopold Löwenheim [65], who proved a version of the theorem that every first-order sentence which is valid in some structure is valid in a countable structure. Löwenheim was working in the framework of the calculus of relations, and his theorem is formulated in that framework. Thoralf Skolem [101] filled a serious gap in Löwenheim's argument, and he extended Löwenheim's theorem by proving that every countable set of first-order sentences that is valid in some structure must be valid in a countable structure. Tarski [102] noted that if a countable set of sentences is valid in some structure, but not in a finite structure, then the set of sentences is valid not only in a structure of countably infinite cardinality, but also in a structure of uncountably infinite cardinality. Thus, this upward version of the Löwenheim-Skolem Theorem is due to Tarski.

The general notions of an elementary substructure and an elementary extension were introduced for arbitrary relational structures by Tarski and Robert Vaught in [114]. Lemmas 6.24, 6.25, and 6.32, and Theorems 6.26 and 6.28 (formulated for arbitrary relational structures) are all from [114].

The results in Exercises 6.1 and 6.3 are due to Andréka-Givant-Németi [5]. The result in Exercise 6.5 is due to Givant (see p. 250 of [113]). The result in Exercise 6.24, in its application to Boolean algebras, dates back at least to Sikorski [99] (see also Sikorski [100]). The result implicit in Exercise 6.21 and the results in Exercises 6.26 and 6.28, as well as Exercises 6.37–6.49, are due to Givant.

Exercises

6.1. Prove that the set of finite subsets and cofinite subsets (complements of finite subsets) of a group G is a subuniverse of the group complex algebra $\mathfrak{Cm}(G)$.

6.2. If P is a projective geometry of finite order, and if ι is the new element that is adjoined to P as an identity element, prove that the set of finite and cofinite subsets of the set $P \cup \{\iota\}$ is a subuniverse of the geometric complex algebra $\mathfrak{Cm}(P)$.

6.3. A group is called *torsion-free* if for each element f different from the group identity element, the integer powers of f are all distinct. Prove that if G is a torsion-free group with identity element e, then every finite or cofinite subset X of G that is different from

$$\varnothing, \qquad \{e\}, \qquad G \sim \{e\}, \qquad \text{and} \qquad G$$

must generate an infinite subalgebra of the complex algebra $\mathfrak{Cm}(G)$.

6.4. Prove that the subuniverse generated by a subset X of a relation algebra $\mathfrak{A}$ is just the set of values of relation algebraic terms on sequences of elements from X.

6.5. Prove that the full set relation algebra on a finite set is always generated by a single element.

6.6. If $\mathfrak{B}$ is a subalgebra of a relation algebra $\mathfrak{A}$, prove that every subalgebra of $\mathfrak{A}$ whose universe is included in $\mathfrak{B}$ must be a subalgebra of $\mathfrak{B}$.

6.7. Complete the proof of Lemma 6.1 by treating the cases when γ is one of terms $\sigma + \tau$, $-\sigma$, and $\sigma^{\smile}$.

6.8. Complete the proof of Lemma 6.2 by treating the cases when Γ is the formula $\Phi \to \Delta$.

6.9. Prove Corollary 6.8 directly, without using Lemma 6.7.

6.10. Let $(\mathfrak{A}_i : i \in I)$ be a directed system of relation algebras, and $\mathfrak{A}$ the union of this system. Prove that an equation in the language of relation algebras is true in $\mathfrak{A}$ if and only if it is true in $\mathfrak{A}_i$ for each i.

6.11. Is the union of a directed system of Boolean relation algebras again a Boolean relation algebra?

6.12. Is the union of a directed system of symmetric algebras again a symmetric relation algebra?

6.13. Is the union of a directed system of group complex algebras again a group complex algebra?

6.14. Is the union of a directed system of geometric complex algebras again a geometric complex algebra?

6.15. Is the union of a directed system of set relation algebras again a set relation algebra?

6.16. Give an example to show that the union of two subalgebras of a relation algebra need not be a subalgebra.

6.17. Prove that a subalgebra $\mathfrak{B}$ of a complete relation algebra $\mathfrak{A}$ is a complete subalgebra if and only if the infimum in $\mathfrak{A}$ of every subset of $\mathfrak{B}$ belongs to $\mathfrak{B}$.

6.18. Prove that the relation of one relation algebra being a complete subalgebra of another is a partial order on the class of all complete relation algebras.

6.19. If $\mathfrak{B}$ is a complete subalgebra of a complete relation algebra $\mathfrak{A}$, and $\mathfrak{C}$ a subalgebra of $\mathfrak{B}$, prove that $\mathfrak{C}$ is a complete subalgebra of $\mathfrak{A}$ if and only if it is a complete subalgebra of $\mathfrak{B}$.

6.20. Prove that the intersection of a system of complete subalgebras of a complete relation algebra $\mathfrak{A}$ is again a complete subalgebra of $\mathfrak{A}$.

6.21. Is the union of a chain of complete subalgebras of a complete relation algebra $\mathfrak{A}$ necessarily a complete subalgebra of $\mathfrak{A}$?

6.22. Prove that the relation of one relation algebra being a regular subalgebra of another is a partial order on the class of all relation algebras.

6.23. Prove that the following conditions on a subalgebra $\mathfrak{B}$ of a relation algebra $\mathfrak{A}$ are equivalent.

(i) $\mathfrak{B}$ is a regular subalgebra of $\mathfrak{A}$.
(ii) For every subset X of $\mathfrak{B}$, if X has an infimum r in $\mathfrak{B}$, then r is also the infimum of X in $\mathfrak{A}$.
(iii) For every subset X of $\mathfrak{B}$, if $\prod X = 0$ in $\mathfrak{B}$, then $\prod X = 0$ in $\mathfrak{A}$.

6.24. A subalgebra $\mathfrak{B}$ of a relation algebra $\mathfrak{A}$ is said to be *dense in* $\mathfrak{A}$ if every non-zero element in $\mathfrak{A}$ is above a non-zero element in $\mathfrak{B}$. Prove that a dense subalgebra is necessarily a regular subalgebra.

6.25. Is the union of a chain of regular subalgebras of a relation algebra $\mathfrak{A}$ necessarily a regular subalgebra of $\mathfrak{A}$?

6.26. Give an example of a complete relation algebra $\mathfrak{A}$ and a relation algebra $\mathfrak{B}$ such that $\mathfrak{B}$ is a regular subalgebra of $\mathfrak{A}$, but not a complete subalgebra of $\mathfrak{A}$. Can you give an example in which $\mathfrak{A}$ is simple?

6.27. If a complete relation algebra $\mathfrak{B}$ is a regular subalgebra of a complete relation algebra $\mathfrak{A}$, prove that $\mathfrak{B}$ must be a complete subalgebra of $\mathfrak{A}$.

6.28. Suppose $\mathfrak{A}$ is a Boolean algebra with quasi-complete (or complete) operators. Prove that every regular subalgebra of $\mathfrak{A}$ must also have quasi-complete (or complete) operators.

6.29. Formulate and prove a version of Theorem 6.18 that applies to arbitrary atomic Boolean algebras with additional operations.

6.30. Prove directly that conditions (i) and (iii) in Lemma 6.19 are equivalent, without using condition (ii).

6.31. Formulate and prove a version of Lemma 6.19 that applies to arbitrary Boolean algebras with additional operations.

6.32. Complete the proof of Atomic Subalgebra Theorem 6.21 by showing that the set B defined in the proof is closed under the operations $+$ and $\smile$.

6.33. Formulate and prove a version of Atomic Subalgebra Theorem 6.21 that applies to Boolean algebras with complete operators of arbitrary ranks.

6.34. Prove the following version of Atomic Subalgebra Theorem 6.21 that applies to Boolean algebras with quasi-complete operators of the same similarity type as relation algebras. Suppose $\mathfrak{A}$ is a Boolean algebra with quasi-complete operators, and W is a subset of $\mathfrak{A}$ with the following properties.

(i) The elements in W are disjoint and sum to 1.
(ii) The element 1' is the sum of the elements in W that are below 1'.
(iii) If p is in $W \cup \{0\}$, then $p^{\smile}$ is the sum of the elements in W that are below $p^{\smile}$.
(iv) If p and q are in $W \cup \{0\}$, then $p\,;q$ is the sum of the elements in W that are below $p\,;q$.

The set of sums $\sum X$ such that X is a subset W and $\sum X$ exists in $\mathfrak{A}$ is then the universe of a regular subalgebra of $\mathfrak{A}$ that is atomic, and the atoms of this subalgebra are just the non-zero elements in W. If, in addition, $\mathfrak{A}$ is complete, then the subalgebra is a complete subalgebra of $\mathfrak{A}$.

6.35. Formulate and prove a version of Atomic Subalgebra Theorem 6.21 that applies to Boolean algebras with quasi-complete operators of arbitrary ranks.

6.36. Complete the computations of the values in Table 6.1 by showing that

$$r_2\,;r_2 = r_2, \qquad r_3\,;r_4 = r_3, \qquad r_4\,;r_4 = r_4, \qquad r_5\,;r_5 = r_5,$$

and

$$r_2\,;r_3 = r_2\,;r_4 = r_2\,;r_5 = r_4\,;r_5 = 0.$$

6.37. Let P be a projective geometry, ι the new element that is adjoined to P as the identity element of $\mathfrak{Cm}(P)$, and Q a subspace of P. Take W to be the set consisting of the subset $P \sim Q$ and the singletons of the individual elements in $Q \cup \{\iota\}$. Prove that W satisfies the conditions of Atomic Subalgebra Theorem 6.21 with respect to the geometric complex algebra $\mathfrak{Cm}(P)$. Describe the elements and atoms in the resulting subalgebra of $\mathfrak{Cm}(P)$.

6.38. Let H be a normal subgroup of a group G, and take W to be the set of cosets of H that are different from H, together with the elements in H. Prove that W satisfies the conditions of Atomic Subalgebra Theorem 6.21 with respect to the relation algebra $\mathfrak{Cm}(G)$. Describe the complete subalgebra of $\mathfrak{Cm}(G)$ that is completely generated by the set W.

6.39. Let $\mathbb{Z}$ be the additive group of the integers, and W the set consisting of $\{0\}$, the set E of non-zero even integers, and the set O of odd integers. Prove that W satisfies the conditions of Atomic Subalgebra Theorem 6.21. Conclude that W generates an eight-element subalgebra of $\mathfrak{Cm}(\mathbb{Z})$ in which the atoms are precisely the elements in W.

6.40. Let $\mathbb{Z}$ be the additive group of the integers, and n an integer greater than 1. Put

$$X_0 = \{m \in \mathbb{Z} : m \equiv 0 \mod n \text{ and } m \neq 0\},$$

and for integers k with $0 \leq k < n$, put

$$X_k = \{m \in \mathbb{Z} : m \equiv k \mod n\}.$$

Let W to be the set consisting of $\{0\}$ and the sets X_k for $0 \leq k < n$. Prove that W satisfies the conditions of Atomic Subalgebra Theorem 6.21 with respect to the complex algebra $\mathfrak{Cm}(\mathbb{Z})$. Conclude that W generates a subalgebra of $\mathfrak{Cm}(\mathbb{Z})$ of cardinality 2^{n+1} in which the atoms are precisely the elements in W. Notice that this exercise generalizes the construction in Exercise 6.39. Notice also that the algebra is closely related to the complex algebra of the group of integers modulo n, but the two algebras are not the same, and in fact they don't even have the same cardinality.

6.41. Let H be a non-trivial normal subgroup of a group G. Take W to be the set consisting of singleton of the group identity element ι, the set $H \sim \{\iota\}$, and the cosets of H that are different from H. Prove that W satisfies the conditions of Atomic Subalgebra Theorem 6.21 with respect to the complex algebra $\mathfrak{Cm}(G)$. Describe the complete and atomic subalgebra of $\mathfrak{Cm}(G)$ that is completely generated by the set W. This exercise generalizes Exercise 6.40.

6.42. Let G be a group and H a non-trivial normal subgroup of G. Write $\mathfrak{A}_H$ for the complete subalgebra of $\mathfrak{Cm}(G)$ described in Exercise 6.41. Suppose K is a non-trivial normal subgroup of G that is included in H and has index κ in H (that is to say, K has κ cosets in H). Prove that $\mathfrak{A}_H$ is a complete subalgebra of $\mathfrak{A}_K$ and that every atom in $\mathfrak{A}_H$ different from the identity atom ι is the sum of κ atoms in $\mathfrak{A}_K$.

6.43. Let $\mathbb{Z}$ be the additive group of the integers, and W the collection of subsets of $\mathbb{Z}$ of the form $\{-n, n\}$ for $n = 0, 1, 2, \ldots$. Prove that W satisfies the conditions of Atomic Subalgebra Theorem 6.21. Conclude that the collection of sets of the form $\bigcup X$, for subsets X of W, is the universe of a complete and atomic subalgebra $\mathfrak{A}$ of $\mathfrak{Cm}(\mathbb{Z})$, and that the atoms in $\mathfrak{A}$ are just the elements in W. Observe that the elements in $\mathfrak{A}$ are precisely the symmetric elements in $\mathfrak{Cm}(\mathbb{Z})$.

6.44. Let $\mathbb{Z}$ be the additive group of the integers. For each integer n, define R_n to be the function (and hence binary relation) on $\mathbb{Z}$ that maps each integer m to the integer $m + n$. Take W to be the set of relations R_n for n in $\mathbb{Z}$. Prove that W satisfies the conditions of Atomic Subalgebra Theorem 6.21 with respect to the full set relation algebra $\mathfrak{Re}(\mathbb{Z})$. Describe the complete subalgebra of $\mathfrak{Re}(\mathbb{Z})$ that is completely generated by W.

6.45. Let $\mathfrak{A}$ be the complete subalgebra of $\mathfrak{Re}(\mathbb{Z})$ constructed in the preceding exercise (where $\mathbb{Z}$ is the additive group of integers), and fix an integer $k \geq 2$. Write $k\mathbb{Z}$ for the subgroup of $\mathbb{Z}$ consisting of the multiples of k, and for each integer i with $0 \leq i < k$, write $k\mathbb{Z} + i$ for the coset of $k\mathbb{Z}$ obtained by adding i to each integer in $k\mathbb{Z}$. Take W to be the set of restrictions of atoms in $\mathfrak{A}$ to cosets of $k\mathbb{Z}$. Thus, for each integer n and each integer i with $0 \leq i < k$, the restriction of the relation R_n (defined in Exercise 6.44) to the coset $k\mathbb{Z}+i$ is an element in W, and every element in W has this form. Prove that W satisfies the conditions of Atomic Subalgebra Theorem 6.21 with respect to the full set relation algebra $\mathfrak{Re}(\mathbb{Z})$. Describe the complete subalgebra of $\mathfrak{Re}(\mathbb{Z})$ that is completely generated by W. If $\mathfrak{A}_k$ is this subalgebra, prove that $\mathfrak{A}$ is a complete subalgebra of $\mathfrak{A}_k$, and that every atom in $\mathfrak{A}$ is the sum of k atoms in $\mathfrak{A}_k$.

6.46. Consider the algebras $\mathfrak{A}_k$ constructed in the preceding exercise. Prove that $\mathfrak{A}_k$ is a subalgebra, and hence a complete subalgebra, of $\mathfrak{A}_\ell$

if and only if k divides ℓ. Prove further that if $\ell = km$, then every atom in $\mathfrak{A}_k$ is the sum of m atoms in $\mathfrak{A}_\ell$.

6.47. Give an example to show that a subalgebra of an atomic relation algebra can be atomless. (Compare this with the result in Theorem 6.18.)

6.48. Give an example to show that a subalgebra of a simple, atomic relation algebra can be atomless.

6.49. Give an example to show that a subalgebra of an infinite integral relation algebra (see Exercise 3.20) can have exactly one atom. (It will be shown in Section 9.2 that the identity element is always an atom in an integral relation algebra.)

6.50. Prove that the relation of one relation algebra being an elementary subalgebra of another is a partial order on the class of all relation algebras.

6.51. Formulate and prove a version of the downward Löwenheim-Skolem-Tarski Theorem 6.26 that applies to arbitrary relational structures.

6.52. Formulate and prove a version of the upward Löwenheim-Skolem-Tarski Theorem 6.28 that applies to arbitrary relational structures.

6.53. Formulate and prove a version of Lemma 6.32 that applies to arbitrary relational structures.

Chapter 7
Homomorphisms

Two algebras with the same intrinsic structure are often identified in mathematics, even though the elements in the two algebras may in fact be different. The way of making this identification precise is via the notion of an isomorphism. More generally, two algebras may bear a structural resemblance to one another, even though they do not have exactly the same intrinsic structure. Homomorphisms provide a tool for establishing structural similarities. Because the notion of a homomorphism is more general than that of an isomorphism, we discuss it first. It is general algebraic in nature, and applies to arbitrary algebras, not just to relation algebras.

7.1 Homomorphisms

Let $\mathfrak{A}$ and $\mathfrak{B}$ be algebras of the same similarity type as relation algebras. A *homomorphism* from $\mathfrak{A}$ to $\mathfrak{B}$ is defined to be a mapping φ from $\mathfrak{A}$ into $\mathfrak{B}$ (or, more precisely, from the universe of $\mathfrak{A}$ into the universe of $\mathfrak{B}$) that *preserves the operations* of $\mathfrak{A}$ in the sense that

$$\varphi(r + s) = \varphi(r) + \varphi(s), \qquad \varphi(-r) = -\varphi(r),$$
$$\varphi(r\,;s) = \varphi(r)\,;\varphi(s), \qquad \varphi(r^{\smile}) = \varphi(r)^{\smile}$$

for all elements r and s in $\mathfrak{A}$, and $\varphi(1\text{'}) = 1\text{'}$. (The operations on the left sides of the equations are those of $\mathfrak{A}$, while the ones on the right sides are those of $\mathfrak{B}$.) The algebras $\mathfrak{A}$ and $\mathfrak{B}$ are respectively called the *domain algebra* and the *target algebra* of the homomorphism. A homomorphism that maps $\mathfrak{A}$ onto $\mathfrak{B}$ is called an *epimorphism*, and

S. Givant, *Introduction to Relation Algebras*,
DOI 10.1007/978-3-319-65235-1_7

one that maps $\mathfrak{A}$ one-to-one into $\mathfrak{B}$ is called a *monomorphism*, or an *embedding*. A homomorphism that is both one-to-one and onto is called an *isomorphism*. If there is a homomorphism φ from $\mathfrak{A}$ onto $\mathfrak{B}$, then $\mathfrak{B}$ is said to be a *homomorphic image* of $\mathfrak{A}$, and in this case $\mathfrak{B}$ is called the *range algebra* or *image algebra* of the homomorphism; if φ is also one-to-one and therefore an isomorphism, then $\mathfrak{B}$ is said to be an *isomorphic image* of $\mathfrak{A}$, and $\mathfrak{A}$ and $\mathfrak{B}$ are said to be *isomorphic*. A homomorphism with domain algebra $\mathfrak{A}$ is said to be a homomorphism *on* $\mathfrak{A}$.

A homomorphism φ is called an *extension* of a homomorphism ψ, and ψ is called a *restriction* of φ, if the domain of ψ is a subalgebra of the domain of φ and if φ and ψ agree on the elements in the domain of ψ.

The composition of a homomorphism from $\mathfrak{A}$ to $\mathfrak{B}$ with a homomorphism from $\mathfrak{B}$ to $\mathfrak{C}$ is easily seen to be a homomorphism from $\mathfrak{A}$ to $\mathfrak{C}$. Moreover, if both homomorphisms are onto, or both are one-to-one, then so is the composition. In particular, the composition of an isomorphism from $\mathfrak{A}$ to $\mathfrak{B}$ with an isomorphism from $\mathfrak{B}$ to $\mathfrak{C}$ is an isomorphism from $\mathfrak{A}$ to $\mathfrak{C}$. The inverse of an isomorphism from $\mathfrak{A}$ to $\mathfrak{B}$ is of course an isomorphism from $\mathfrak{B}$ to $\mathfrak{A}$. All these assertions are easily checked and are left to the reader.

The equational nature of axioms (R1)–(R10) implies that every homomorphic image of a relation algebra is again a relation algebra. In more detail, suppose $\mathfrak{A}$ is a relation algebra and φ a homomorphism from $\mathfrak{A}$ onto some algebra $\mathfrak{B}$. To see that the second involution law holds in $\mathfrak{B}$, let u and v be arbitrary elements in $\mathfrak{B}$. Since φ is assumed to be onto, there must be elements r and s in $\mathfrak{A}$ that are mapped by φ to u and v respectively. The second involution law holds in $\mathfrak{A}$, by assumption, so

$$(r\,;s)^{\smile} = s^{\smile}\,;r^{\smile}\,.$$

Apply the homomorphism φ to both sides of this equation, and use the assumptions about r and s, and the homomorphism properties of φ, to obtain

$$\begin{aligned}(u\,;v)^{\smile} = (\varphi(r)\,;\varphi(s))^{\smile} &= \varphi((r\,;s)^{\smile}) \\ &= \varphi(s^{\smile}\,;r^{\smile}) = \varphi(s)^{\smile}\,;\varphi(r)^{\smile} = v^{\smile}\,;u^{\smile}\,.\end{aligned}$$

Similar arguments show that the other relation algebraic axioms hold in $\mathfrak{B}$ as well.

A mapping φ from a relation algebra $\mathfrak{A}$ into a relation algebra $\mathfrak{B}$ that preserves the Boolean operations of $\mathfrak{A}$, but not necessarily the Peircean operations, is called a *Boolean* homomorphism. Analogously, if φ preserves the Peircean operations of $\mathfrak{A}$ (including the identity element), but not necessarily the Boolean operations, then φ is called a *Peircean* homomorphism. If a Boolean or Peircean homomorphism is onto, or one-to-one, or both, then we may replace the term "homomorphism" by "epimorphism", or "monomorphism", or "isomorphism" respectively, speaking for example of a Boolean or a Peircean isomorphism. In the sequel, when speaking simply of a homomorphism, we shall always mean a homomorphism from one relation algebra into another, unless explicitly stated otherwise. If necessary, we shall speak of a *relation algebra homomorphism* to clarify the situation.

7.2 Properties preserved under homomorphisms

Homomorphisms preserve not only the fundamental relation algebraic operations, but also the operations that are definable by terms in the language $\mathcal{L}$ of relation algebras.

Lemma 7.1. *Let $\gamma(v_0, \ldots, v_{n-1})$ be a term in the language of relation algebras, and φ a homomorphism from $\mathfrak{A}$ to $\mathfrak{B}$. For every sequence of elements $r_0, \ldots, r_{n-1}$ in $\mathfrak{A}$, we have*

$$\varphi(\gamma(r_0, \ldots, r_{n-1})) = \gamma(\varphi(r_0), \ldots, \varphi(r_{n-1})).$$

Proof. The proof proceeds by induction on terms. There are two base cases to consider. If γ is a variable v_i, then

$$\varphi(\gamma(r_0, \ldots, r_{n-1})) = \varphi(r_i) = \gamma(\varphi(r_0), \ldots, \varphi(r_{n-1})),$$

by the definition of the value of a term on a sequence of elements. (The operations on the left and right sides of this equation are the ones induced by γ in $\mathfrak{A}$ and in $\mathfrak{B}$ respectively.) A similar argument applies if γ is the individual constant symbol 1'.

Assume now as the induction hypothesis that the operations induced by terms σ and τ are preserved by φ in the sense of the lemma. There are four cases to consider. If γ is the term $\sigma ; \tau$, then

$$\begin{aligned}\varphi(\gamma(r_0,\dots,r_{n-1})) &= \varphi(\sigma(r_0,\dots,r_{n-1}) \mathbin{;} \tau(r_0,\dots,r_{n-1}))\\ &= \varphi(\sigma(r_0,\dots,r_{n-1})) \mathbin{;} \varphi(\tau(r_0,\dots,r_{n-1}))\\ &= \sigma(\varphi(r_0),\dots,\varphi(r_{n-1})) \mathbin{;} \tau(\varphi(r_0),\dots,\varphi(r_{n-1}))\\ &= \gamma(\varphi(r_0),\dots,\varphi(r_{n-1})).\end{aligned}$$

The first and last equalities use the assumption on the form of γ and the definition of the value of a term on a sequence of elements. The second equality uses the assumption that φ is a homomorphism and therefore preserves the operation $\mathbin{;}$. The third equality uses the induction hypothesis that φ preserves the operations induced by the terms σ and τ. Thus, the conclusion of the lemma holds in this case. A similar argument applies if γ is one of the terms $\sigma + \tau$, or $-\sigma$, or $\sigma^{\smile}$. The principle of induction for terms now yields the desired conclusion. □

Homomorphisms preserve positive algebraic properties, that is to say, they preserve properties that can be expressed by positive formulas (see Section 2.4). In particular, homomorphisms preserve all equations. To formulate this result precisely, it is helpful to introduce a bit of notation. If r is a sequence of elements in an algebra $\mathfrak{A}$, say

$$r = (r_0, \dots, r_{n-1}),$$

and if φ is a homomorphism from $\mathfrak{A}$ into $\mathfrak{B}$, then write $\varphi(r)$ for the image of r under φ, so that

$$\varphi(r) = (\varphi(r_0), \dots, \varphi(r_{n-1})).$$

Lemma 7.2. *If φ is a homomorphism from $\mathfrak{A}$ onto $\mathfrak{B}$, then for every positive formula Γ and every appropriate sequence r of elements in $\mathfrak{A}$, if r satisfies Γ in $\mathfrak{A}$, then the sequence $\varphi(r)$ satisfies Γ in $\mathfrak{B}$.*

Proof. The proof proceeds by induction on positive formulas. For the base case, assume that Γ is an equation, say $\sigma = \tau$. Suppose

$$\sigma(r) = \tau(r)$$

in $\mathfrak{A}$. Apply φ to both sides of this equation to obtain

$$\varphi(\sigma(r)) = \varphi(\tau(r)).$$

Use Lemma 7.1 to conclude that

$$\sigma(\varphi(r)) = \tau(\varphi(r)).$$

Thus, $\varphi(r)$ satisfies Γ in $\mathfrak{B}$, as desired.

Assume now as the induction hypothesis that the lemma holds for formulas Δ and Φ. Consider the case when Γ is the disjunction $\Delta \vee \Phi$. If r satisfies Γ in $\mathfrak{A}$, then r must satisfy at least one of Δ and Φ in $\mathfrak{A}$, by the definition of satisfaction. The induction hypothesis therefore implies that $\varphi(r)$ must satisfy at least one of Δ and Φ in $\mathfrak{B}$. Use the definition of satisfaction again to conclude that $\varphi(r)$ satisfies Γ in $\mathfrak{B}$. An analogous argument applies when Γ is the conjunction of Δ and Φ.

Turn now to the case when Γ is obtained from Δ by existential quantification. For notational simplicity, it may be assumed that Γ has the form $\exists v_0 \Delta(v_0, \ldots, v_n)$, and

$$r = (r_1, \ldots, r_n). \tag{1}$$

If r satisfies Γ in $\mathfrak{A}$, then there must be an element r_0 in $\mathfrak{A}$ such that the sequence

$$(r_0, r_1, \ldots, r_n). \tag{2}$$

satisfies Δ in $\mathfrak{A}$, by the definition of satisfaction. The induction hypothesis on Δ implies that the sequence

$$(\varphi(r_0), \varphi(r_1), \ldots \varphi(r_n)) \tag{3}$$

satisfies Δ in $\mathfrak{B}$. Use the definition of satisfaction again to conclude that $\varphi(r)$ satisfies Γ in $\mathfrak{B}$.

There remains the case when Γ is obtained from Δ by universal quantification. For notational simplicity. it may be assumed that Γ has the form $\forall v_0 \Delta(v_0, \ldots, v_n)$ and r is determined as in (1). If r satisfies Γ in $\mathfrak{A}$, then for all elements r_0 in $\mathfrak{A}$, the sequence (2) must satisfy Δ in $\mathfrak{A}$, by the definition of satisfaction. The induction hypothesis on Δ implies that the sequence (3) satisfies Δ in $\mathfrak{B}$. The homomorphism φ is assumed to map $\mathfrak{A}$ onto $\mathfrak{B}$, so every element in $\mathfrak{B}$ has the form $\varphi(r_0)$ for some element r_0 in $\mathfrak{A}$. Use this observation and the definition of satisfaction to conclude that $\varphi(r)$ satisfies Γ in $\mathfrak{B}$. The conclusion of the lemma now follows by the principle of induction for positive formulas. □

The assumption in the preceding lemma that φ maps $\mathfrak{A}$ onto $\mathfrak{B}$ is only used in the induction step for universal quantification. Consequently, for positive formulas without universal quantifiers, the lemma is true even when φ does not map $\mathfrak{A}$ onto $\mathfrak{B}$.

Corollary 7.3. *If a positive formula Γ is true in an algebra $\mathfrak{A}$, then Γ is true in all homomorphic images of $\mathfrak{A}$.*

It follows from the preceding discussion that homomorphisms preserve all operations and relations on the universe of a relation algebra that are definable by means of positive formulas. For example, homomorphisms automatically preserve the operations of multiplication and relative addition, and they also preserve the distinguished constants zero, one, and the diversity element, because these operations and distinguished constants are defined by means of terms in the language of relation algebras (see Lemma 7.1).

Also, inequalities are preserved by a homomorphism φ in the sense that

$$r \le s \qquad \text{implies} \qquad \varphi(r) \le \varphi(s),$$

because the relation $\le$ is defined in terms of addition by a positive formula. The converse that $\varphi(r) \le \varphi(s)$ implies $r \le s$ fails in general for homomorphisms and even for epimorphisms, but it holds when φ is a monomorphism. In more detail, if $\varphi(r) \le \varphi(s)$, then

$$\varphi(r) + \varphi(s) = \varphi(s),$$

by the definition of $\le$, and therefore

$$\varphi(r + s) = \varphi(s),$$

by the homomorphism properties of φ. For a monomorphism φ, it follows that $r + s = s$ and therefore $r \le s$.

Other examples of positive properties that are preserved under the passage to homomorphic images are all of the properties of individual elements discussed in Chapter 5, because these properties are defined by means of equations. For example, if r is an equivalence element, or an ideal element, or a function, or a rectangle in a relation algebra, then the image of r under a homomorphism must also possess this property in the image algebra. These observations also apply to sequences of elements. For example, if two elements r and s in a relation algebra $\mathfrak{A}$ commute, then the images of these two elements under a homomorphism must also commute in the image algebra; and if an element r in $\mathfrak{A}$ satisfies the distributive law for relative multiplication over multiplication in the sense that the equation

$$r \,;(s \cdot t) = (r \,; s) \cdot (r \,; t)$$

holds for all elements s and t in $\mathfrak{A}$, then for every epimorphism φ from $\mathfrak{A}$ to an algebra $\mathfrak{B}$, the image of r under φ must satisfy the same distributive law in $\mathfrak{B}$. Analogous remarks hold for properties that apply to entire relation algebras. For example, if $\mathfrak{A}$ is a commutative or a symmetric relation algebra, then so is every homomorphic image of $\mathfrak{A}$.

Algebraic properties that are not positive are usually not preserved by homomorphisms. For example, the homomorphic image of an atomless relation algebra need not be atomless; in fact, the image can be atomic. Similarly, the property of a specific element being an atom in a relation algebra is not preserved by homomorphisms, since an atom may be mapped to zero by a homomorphism.

There are also important properties of sets of elements that are preserved under homomorphisms. An example is the property of being a subuniverse: the homomorphic image of a subuniverse is again a subuniverse, and so is the inverse homomorphic image of a subuniverse.

Lemma 7.4. *Let φ be a homomorphism from a relation algebra $\mathfrak{A}$ into a relation algebra $\mathfrak{B}$. If C is a subuniverse of $\mathfrak{A}$, then the image set*

$$\varphi(C) = \{\varphi(r) : r \in C\}$$

is a subuniverse of $\mathfrak{B}$. Similarly, if D is a subuniverse of $\mathfrak{B}$, then the inverse image set

$$\varphi^{-1}(D) = \{r \in A : \varphi(r) \in D\}$$

is a subuniverse of $\mathfrak{A}$.

Proof. The subuniverse C contains the identity element of $\mathfrak{A}$, by assumption, and φ maps this identity element to the identity element of $\mathfrak{B}$, by the definition of a homomorphism, so the identity element of $\mathfrak{B}$ belongs to $\varphi(C)$. If u and v are elements in $\varphi(C)$, then there must be elements r and s in C that are mapped to u and v respectively, by the definition of the image set $\varphi(C)$. The elements

$$r + s, \qquad -r, \qquad r \mathbin{;} s, \qquad r^{\smile}$$

all belong to C, by assumption, so the images of these elements belong to $\varphi(C)$. The homomorphism properties of φ imply that these images are just the elements

$$u + v, \qquad -u, \qquad u\,;v, \qquad u^{\smile}$$

respectively, so $\varphi(C)$ is closed under the operations of $\mathfrak{B}$ and is consequently a subuniverse of $\mathfrak{B}$. This proves the first assertion of the lemma. The second is proved in an analogous fashion. □

Corollary 7.5. *A homomorphism from a relation algebra* $\mathfrak{A}$ *into a relation algebra* $\mathfrak{B}$ *maps the minimal subalgebra of* $\mathfrak{A}$ *homomorphically onto the minimal subalgebra of* $\mathfrak{B}$.

Proof. Let C and D be the universes of the minimal subalgebras of $\mathfrak{A}$ and $\mathfrak{B}$ respectively. The image set $\varphi(C)$ is a subuniverse of $\mathfrak{B}$, by the first part of Lemma 7.4, and D is the minimal subuniverse of $\mathfrak{B}$, so D is included in $\varphi(C)$. Similarly, the inverse image set $\varphi^{-1}(D)$ is a subuniverse of $\mathfrak{A}$, by the second part of Lemma 7.4, and C is the minimal subuniverse of $\mathfrak{A}$, so C is included in $\varphi^{-1}(D)$. It follows from this last observation that $\varphi(C)$ is included in D, because any element r in C must belong to $\varphi^{-1}(D)$ and therefore $\varphi(r)$ must belong to D. Conclusion: $\varphi(C) = D$. □

The preceding corollary says that a homomorphism maps the subuniverse of $\mathfrak{A}$ generated by the empty set onto the subuniverse of $\mathfrak{B}$ generated by the empty set. For epimorphisms, a more general result is true: the image of a generating set of $\mathfrak{A}$ under an epimorphism is always a generating set of $\mathfrak{B}$.

Lemma 7.6. *Let* φ *be an epimorphism from a relation algebra* $\mathfrak{A}$ *to a relation algebra* $\mathfrak{B}$. *If* X *is a set of generators of* $\mathfrak{A}$, *then the image set*

$$\varphi(X) = \{\varphi(r) : r \in X\}$$

is a set of generators of $\mathfrak{B}$.

Proof. Write Y for the image set $\varphi(X)$. It is to be shown that Y generates $\mathfrak{B}$. Define sequences of sets

$$X_0, X_1, X_2, \ldots \qquad \text{and} \qquad Y_0, Y_1, Y_2, \ldots$$

in terms of X and Y just as is done before Lemma 6.5:

$$X_0 = X \cup \{1'\} \qquad \text{and} \qquad Y_0 = Y \cup \{1'\}, \tag{1}$$

and X_{i+1} and Y_{i+1} are the one-step closures of X_i and Y_i in $\mathfrak{A}$ and $\mathfrak{B}$ respectively (see the remarks preceding Lemma 6.5). We proceed to prove by induction on natural numbers i that

$$\varphi(X_i) = Y_i \tag{2}$$

for each i. For the case $i = 0$, this equality follows immediately from the definitions of X_0 and Y_0 in (1), and from the definition of Y as the image set $\varphi(X)$. Assume now as the induction hypothesis that (2) holds for a given natural number i. If t belongs to the set X_{i+1}, then there must be elements r and s in X_i such that t is equal to one of

$$r + s, \qquad -r, \qquad r \mathbin{;} s, \qquad r^{\smile},$$

by the definition of X_{i+1} as the one-step closure of X_i. Suppose as an example that $t = r \mathbin{;} s$. The elements $u = \varphi(r)$ and $v = \varphi(s)$ belong to Y_i by the induction hypothesis, so the product $w = u \mathbin{;} v$ belongs to the set Y_{i+1}, by the definition of Y_{i+1} as the one-step closure of Y_i. Since

$$\varphi(t) = \varphi(r \mathbin{;} s) = \varphi(r) \mathbin{;} \varphi(s) = u \mathbin{;} v = w, \tag{3}$$

it follows that $\varphi(t)$ belongs to Y_{i+1}. This argument shows that $\varphi(X_{i+1})$ is included in Y_{i+1}.

To establish the reverse inclusion, consider any element w in Y_{i+1}. There must be elements u and v in Y_i such that w is equal to one of

$$u + v, \qquad -u, \qquad u \mathbin{;} v, \qquad u^{\smile},$$

by the definition of Y_{i+1}. Suppose as an example that $w = u \mathbin{;} v$. The induction hypothesis implies that there are elements r and s in X_i which are mapped by φ to u and v respectively. The product $t = r \mathbin{;} s$ belongs to the set X_{i+1}, by the definition of X_{i+1}, so the computation in (3) shows that w belongs to the set $\varphi(X_{i+1})$. Thus, Y_{i+1} is included in $\varphi(X_{i+1})$. This proves (2).

It is easy to see, using (2), that Y generates $\mathfrak{B}$. The universe of $\mathfrak{A}$ is equal to the union of the sets X_i, by Lemma 6.5, and the universe of $\mathfrak{B}$ is the image of the universe of $\mathfrak{A}$ under φ, by the assumption that φ is an epimorphism. Consequently,

$$B = \varphi(A) = \varphi(\textstyle\bigcup_i X_i) = \textstyle\bigcup_i \varphi(X_i) = \textstyle\bigcup_i Y_i,$$

so Y generates $\mathfrak{B}$, by Lemma 6.5. □

If a function φ from a relation algebra $\mathfrak{A}$ into a relation algebra $\mathfrak{B}$ preserves enough operations, so that the remaining operations are definable by positive formulas in terms of the preserved ones, then φ is a homomorphism. Consider, for example, the Boolean operations. A function φ that preserves addition need not preserve complement; but if φ preserves addition and multiplication, and if φ maps 0 to 0, and 1 to 1, then φ does preserve complement, because complement is definable in terms of addition, multiplication, zero, and one by a positive formula:

$$s = -r \quad \text{if and only if} \quad r + s = 1 \text{ and } r \cdot s = 0.$$

If φ actually maps $\mathfrak{A}$ onto $\mathfrak{B}$, then it suffices to show that φ preserves addition and multiplication in order to conclude that φ preserves complement, because complement is definable in terms of these two operations alone by a positive, universally quantified formula:

$$s = -r \quad \text{if and only if} \quad (r + s) \cdot t = t \text{ and } (r \cdot s) + t = t \text{ for all } t.$$

(The assumption that φ is onto is needed because the variable t is universally quantified in this formula.) If φ is in fact a bijection, then it suffices just to show that φ preserves the operation of addition in order to conclude that φ preserves multiplication and complement, because both of these operations are definable in terms of addition alone, albeit not by positive formulas. For example, the relation $\leq$ is defined in terms of addition, and multiplication can be defined in terms of $\leq$ because $t = r \cdot s$ if and only if t is greatest lower bound of r and s.

Consider next the Peircean operations. If a function φ from $\mathfrak{A}$ to $\mathfrak{B}$ preserves the operations of addition, complement, relative multiplication, and the identity element, then φ must preserve the operation of converse, because converse is definable in terms of the other operations by means of a positive formula:

$$s = r^{\smile} \qquad \text{if and only if} \qquad s \,;\, -r + 0\text{'} = 0\text{'} \text{ and } r \,;\, -s + 0\text{'} = 0\text{'},$$

by Lemma 4.15. (This observation demonstrates the advantage of the characterization of converse in Lemma 4.15 over the characterization in Lemma 4.14.) If φ maps $\mathfrak{A}$ onto $\mathfrak{B}$, then φ preserves the identity element whenever it preserves relative multiplication, because the identity element is definable in terms of relative multiplication by a positive formula with a universal quantifier (see Section 4.3).

Combine these observations to arrive at the following conclusions. If a function φ from a relation algebra $\mathfrak{A}$ into a relation algebra $\mathfrak{B}$ preserves the operations of addition, multiplication, and relative multiplication, and also the distinguished constants 0, 1, and 1', then φ is a homomorphism from $\mathfrak{A}$ into $\mathfrak{B}$. If φ maps $\mathfrak{A}$ onto $\mathfrak{B}$, then it suffices to show that φ preserves the operations of addition, multiplication, and relative multiplication in order to conclude that φ is a homomorphism and consequently an epimorphism. If φ maps $\mathfrak{A}$ bijectively to $\mathfrak{B}$, then it suffices to show that φ preserves addition and relative multiplication in order to conclude that φ is a homomorphism and hence an isomorphism.

There is one more remark in this direction that is quite useful: homomorphism are completely determined by their action on a generating set.

Lemma 7.7. *If a set X generates a relation algebra $\mathfrak{A}$, and if φ and ψ are homomorphisms from $\mathfrak{A}$ into $\mathfrak{B}$ such that $\varphi(r) = \psi(r)$ for every r in X, then $\varphi = \psi$.*

Proof. The set C of elements r in $\mathfrak{A}$ such that $\varphi(r) = \psi(r)$ is easily seen to be a subuniverse of $\mathfrak{A}$. Indeed, the identity element 1' belongs to C because both φ and ψ map 1' to the identity element of $\mathfrak{B}$. If r and s are elements in C, then

$$\varphi(r\,;s) = \varphi(r)\,;\varphi(s) = \psi(r)\,;\psi(s) = \psi(r\,;s),$$

by the homomorphism properties of φ and ψ, and the definition of the set C, so $r\,;s$ belongs to C. Thus, C is closed under relative multiplication. Analogous arguments show that C is closed under the remaining operations of $\mathfrak{A}$. The set X is clearly included in C, because the given homomorphisms are assumed to agree on the elements in X. Conclusion: C is a subuniverse of $\mathfrak{A}$ that includes the generating set X, so C must coincide with the universe of $\mathfrak{A}$. The homomorphisms φ and ψ are therefore equal, by the definition of C. □

7.3 A class of examples

We proceed to construct a concrete class of examples of homomorphisms between relation algebras. Let E be any equivalence relation

on a set U, and take $\mathfrak{A}$ to be the full set relation algebra on the relation E, so that $\mathfrak{A} = \mathfrak{Re}(E)$. Fix some set X of equivalence classes of E (not necessarily the set of all equivalence classes of E), and put

$$F = \bigcup\{W \times W : W \in X\} \qquad \text{and} \qquad V = \bigcup X.$$

Thus, F is the restriction of the relation E to the set V that is the union of the equivalence classes in X. Take $\mathfrak{B}$ to be the full set relation algebra on the equivalence relation F, so that $\mathfrak{B} = \mathfrak{Re}(F)$. Define a function φ from $\mathfrak{A}$ into $\mathfrak{B}$ by

$$\varphi(R) = R \cap F$$

for all relations R in $\mathfrak{A}$. The function φ clearly preserves the operations of union and intersection, and it maps the unit E and the zero $\varnothing$ of $\mathfrak{A}$ to the unit F and the zero $\varnothing$ of $\mathfrak{B}$ respectively, so φ must preserve the operation of complement as well (see the remarks near the end of Section 7.2). Also, φ clearly maps the identity element id_U to the identity element id_V. To check that φ preserves the operation of relational composition, observe that the relation F is an ideal element in the algebra $\mathfrak{A}$ (see Section 5.5), so

$$(R \,|\, S) \cap F = (R \cap F) \,|\, (S \cap F)$$

for all relations R and S in $\mathfrak{A}$, by the distributive law for ideal elements in Lemma 5.44. Using this equality, we obtain

$$\varphi(R \,|\, S) = (R \,|\, S) \cap F = (R \cap F) \,|\, (S \cap F) = \varphi(R) \,|\, \varphi(S),$$

which shows that φ preserves relational composition. It follows from these observations and those of the previous section that φ is a homomorphism from $\mathfrak{A}$ into $\mathfrak{B}$. In fact, since every relation in $\mathfrak{B}$ is also a relation in $\mathfrak{A}$, and since φ maps every relation in $\mathfrak{B}$ to itself, it may be concluded that φ is an epimorphism.

A special case of the preceding construction occurs when X consists of a single equivalence class V of the relation E. In this case, the mapping φ defined above maps the full set relation algebra on the relation E homomorphically onto the full set relation on the set V.

7.4 Complete homomorphisms

An isomorphism between relation algebras preserves every infinite supremum and infimum that happens to exist, but in general a mere

homomorphism will not do so. A homomorphism φ from $\mathfrak{A}$ to $\mathfrak{B}$ is called *complete* if it preserves all suprema (and consequently all infima) that happen to exist. This means that if a set X of elements in $\mathfrak{A}$ has a supremum s, then the image of X under φ, that is to say, the set

$$\varphi(X) = \{\varphi(r) : r \in X\}$$

has a supremum in $\mathfrak{B}$, and that supremum is $\varphi(s)$, in symbols,

$$\varphi(s) = \sum \varphi(X) = \sum\{\varphi(r) : r \in X\}.$$

A complete monomorphism is also called a *complete embedding.* If there is a complete homomorphism from $\mathfrak{A}$ onto $\mathfrak{B}$, then $\mathfrak{B}$ is said to be a *complete homomorphic image* of $\mathfrak{A}$.

The homomorphism φ from $\mathfrak{Re}(E)$ to $\mathfrak{Re}(F)$ that is discussed in Section 7.3 is an example of a complete homomorphism. For the proof that φ preserves arbitrary sums, consider an arbitrary set Y of relations in $\mathfrak{Re}(E)$, and write $R = \bigcup Y$. We have

$$\begin{aligned}\varphi(R) = R \cap F = (\bigcup Y) \cap F& \\ &= \bigcup\{S \cap F : S \in Y\} = \bigcup\{\varphi(S) : S \in Y\}\end{aligned}$$

by the definition of φ, the definition of R, and the distributivity of intersections over arbitrary unions. Since suprema in $\mathfrak{Re}(E)$ and $\mathfrak{Re}(F)$ are just unions, this argument shows that φ preserves all existing suprema.

It is not difficult to see that the composition of two complete homomorphisms is again a complete homomorphism.

Lemma 7.8. *If φ is a complete homomorphism from $\mathfrak{A}$ to $\mathfrak{B}$, and ψ a complete homomorphism from $\mathfrak{B}$ to $\mathfrak{C}$, then the composition $\psi \circ \varphi$ is a complete homomorphism from $\mathfrak{A}$ to $\mathfrak{C}$.*

Proof. The composition of two homomorphisms is again a homomorphism, so the composition $\vartheta = \psi \circ \varphi$ is a homomorphism from $\mathfrak{A}$ to $\mathfrak{C}$. It remains to check that ϑ is complete. To this end, consider a subset X of $\mathfrak{A}$ for which the supremum, say s, exists in $\mathfrak{A}$. The homomorphism φ is assumed to be complete, so the image set

$$Y = \varphi(X) = \{\varphi(r) : r \in X\}$$

has a supremum in $\mathfrak{B}$, and that supremum is the element $t = \varphi(s)$. The homomorphism ψ is also complete, so the image set

$$\psi(Y) = \{\psi(p) : p \in Y\} = \{\psi(\varphi(r)) : r \in X\}$$
$$= \{\vartheta(r) : r \in X\} = \vartheta(X)$$

has a supremum in $\mathfrak{C}$, and that supremum is

$$\psi(t) = \psi(\varphi(s)) = \vartheta(s).$$

Combine these observations to conclude that the image set $\vartheta(X)$ has a supremum in $\mathfrak{C}$, and that supremum is $\vartheta(s)$. Consequently, the homomorphism ϑ is complete. □

There is an interesting connection between complete monomorphisms and regular subalgebras: a monomorphism is complete if and only if its image algebra is a regular subalgebra.

Lemma 7.9. *A monomorphism φ from $\mathfrak{A}$ into $\mathfrak{B}$ is complete if and only if the image of $\mathfrak{A}$ under φ is a regular subalgebra of $\mathfrak{B}$.*

Proof. The image of $\mathfrak{A}$ under the monomorphism φ is certainly a subalgebra of $\mathfrak{B}$, by Lemma 7.4. Denote this subalgebra by $\mathfrak{C}$, and observe that φ is an isomorphism from $\mathfrak{A}$ to $\mathfrak{C}$. Assume first that $\mathfrak{C}$ is a regular subalgebra of $\mathfrak{B}$. To prove that the monomorphism φ is complete, consider an arbitrary subset X of $\mathfrak{A}$ with a supremum s. Since φ is an isomorphism from $\mathfrak{A}$ to $\mathfrak{C}$, the supremum of the set

$$Y = \{\varphi(r) : r \in X\}$$

in $\mathfrak{C}$ must be $\varphi(s)$. Since $\mathfrak{C}$ is a regular subalgebra of $\mathfrak{B}$, the element $\varphi(s)$ must also be the supremum of Y in $\mathfrak{B}$. Consequently, φ is a complete monomorphism from $\mathfrak{A}$ into $\mathfrak{B}$.

To establish the reverse implication, assume that the monomorphism φ is complete, with the goal of showing that $\mathfrak{C}$ is a regular subalgebra of $\mathfrak{B}$. Consider an arbitrary subset Y of $\mathfrak{C}$ with a supremum t in $\mathfrak{C}$. It is to be shown that t is the supremum of Y in $\mathfrak{B}$. Since φ is an isomorphism from $\mathfrak{A}$ to $\mathfrak{C}$, there is a uniquely determined subset X of $\mathfrak{A}$ and a uniquely determined element s in $\mathfrak{A}$ such that φ maps X bijectively to Y, and $\varphi(s) = t$. The isomorphism properties of φ imply that s must be the supremum of the set X in $\mathfrak{A}$. The completeness of φ ensures that $\varphi(s)$ is the supremum of Y in $\mathfrak{B}$, and this directly implies the desired conclusion that t is the supremum of Y in $\mathfrak{B}$. □

There is a version of Lemma 7.7 that applies to complete homomorphisms.

Lemma 7.10. *If a set X completely generates a complete relation algebra $\mathfrak{A}$, and if φ and ψ are complete homomorphisms from $\mathfrak{A}$ into a relation algebra $\mathfrak{B}$ such that $\varphi(r) = \psi(r)$ for all r in X, then $\varphi = \psi$.*

Proof. Take C to be the set of elements in $\mathfrak{A}$ on which the complete homomorphisms φ and ψ agree. The proof of Lemma 7.7 shows that C is a subuniverse of $\mathfrak{A}$ and X is a subset of C. In fact, C is a complete subuniverse of $\mathfrak{A}$. To see this, consider an arbitrary subset Y of C, and let r be the supremum of the set Y in $\mathfrak{A}$; this supremum exists because $\mathfrak{A}$ is complete. The assumed completeness of φ and ψ, and the fact that these two homomorphisms agree on elements in C (and therefore on elements in Y) imply that

$$\begin{aligned} \varphi(r) = \varphi(\textstyle\sum Y) &= \textstyle\sum\{\varphi(s) : s \in Y\} \\ &= \textstyle\sum\{\psi(s) : s \in Y\} = \psi(\textstyle\sum Y) = \psi(r). \end{aligned}$$

Consequently, r belongs to the set C.

Turn now to the assertion of the lemma. The set X is assumed to completely generate the algebra $\mathfrak{A}$, and the set C is a complete subuniverse of $\mathfrak{A}$ that includes X. Consequently, C must coincide with the universe of $\mathfrak{A}$, and therefore φ must equal ψ, by the definition of C. □

7.5 Isomorphisms

The relation of one relation algebra being isomorphic to another is an equivalence relation on the class of all relation algebras. Indeed, every relation algebra $\mathfrak{A}$ is isomorphic to itself, because the identity function on the universe of $\mathfrak{A}$ is an isomorphism; if φ is an isomorphism from $\mathfrak{A}$ to $\mathfrak{B}$, then the inverse of φ is an isomorphism from $\mathfrak{B}$ to $\mathfrak{A}$; and if φ is an isomorphism from $\mathfrak{A}$ to $\mathfrak{B}$, and ψ an isomorphism from $\mathfrak{B}$ to $\mathfrak{C}$, then the composition $\psi \circ \varphi$ is an isomorphism from $\mathfrak{A}$ to $\mathfrak{C}$. Algebras in the same equivalence class of this relation are said to have the same *isomorphism type* and are often treated as if they were the same algebra, at least from an algebraic point of view. We occasionally write $\mathfrak{A} \cong \mathfrak{B}$ to express that algebras $\mathfrak{A}$ and $\mathfrak{B}$ are isomorphic.

Isomorphisms preserve all intrinsic properties of algebras. They also preserve all intrinsic properties of elements, of sets of elements, and of relations between elements and sets of elements, in the algebras. Here are some examples. Suppose φ is an isomorphism from $\mathfrak{A}$ to $\mathfrak{B}$. The algebras $\mathfrak{A}$ and $\mathfrak{B}$ obviously must have the same cardinality; and $\mathfrak{A}$ will be atomic, or atomless, or complete if and only if $\mathfrak{B}$ is atomic, or atomless, or complete respectively. An element r is an atom in $\mathfrak{A}$ if and only if $\varphi(r)$ is an atom in $\mathfrak{B}$. More generally, for any formula $\Gamma(v_0, \dots, v_{n-1})$ in the language of relation algebras, a sequence $(r_0, \dots, r_{n-1})$ of elements from $\mathfrak{A}$ satisfies Γ in $\mathfrak{A}$ if and only if the image sequence $(\varphi(r_0), \dots, \varphi(r_{n-1}))$ satisfies Γ in $\mathfrak{B}$. A subset X of $\mathfrak{A}$ is a subuniverse, or a generating set, of $\mathfrak{A}$ if and only if the image set $\varphi(X) = \{\varphi(r) : r \in X\}$ is a subuniverse, or a generating set, of $\mathfrak{B}$ respectively. An element r is the supremum or infimum of a subset X in $\mathfrak{A}$ if and only if $\varphi(r)$ is the supremum or infimum of the image set $\varphi(X)$ in $\mathfrak{B}$. And so on.

The fact that isomorphisms preserve all algebraic properties can be used to demonstrate that two relation algebras are not isomorphic. To this end, it suffices to formulate an algebraic property of one of the two algebras that is not shared by the other. For example, the complex algebra of the group of integers cannot be isomorphic to the complex algebra of the group of real numbers because the set of atoms in the former has cardinality strictly smaller than the set of atoms in the latter. Nor can the complex algebra of the group of integers be isomorphic to the full algebra of binary relations on some (infinite) set because relative multiplication is a commutative operation in the former algebra, but not in the latter.

Here is a useful class of examples of isomorphisms between relation algebras. Consider sets U and V of the same cardinality, and let ϑ be a bijection from U to V. Define a mapping φ on the set of all relations on U by putting

$$\varphi(R) = \{(\vartheta(\alpha), \vartheta(\beta)) : (\alpha, \beta) \in R\}$$

for every relation R on U. It is an easy matter to check that φ maps the set of all relations on U bijectively to the set of all relations on V. In fact, if ψ is the mapping on the set of all relations on V that is defined by

$$\psi(T) = \{(\vartheta^{-1}(\alpha), \vartheta^{-1}(\beta)) : (\alpha, \beta) \in T\}$$

for every relation T on V, then the compositions $\varphi \circ \psi$ and $\psi \circ \varphi$ are easily seen to be the identity functions on their respective domains. Consequently, φ is a bijection and ψ is its inverse.

The mapping φ preserves all operations on binary relations, all relations between binary relations, and all distinguished binary relations that are intrinsically definable. For example, to see that relational composition is preserved by φ, consider relations R and S on U. Let α and β be elements in U, and write $\delta = \vartheta(\alpha)$ and $\zeta = \vartheta(\beta)$. The definition of φ, the definition of relational composition, and the assumption that ϑ is a bijection imply that the following six statements are equivalent:

$(\delta, \zeta) \in \varphi(R \mid S)$,
$(\alpha, \beta) \in R \mid S$,
$(\alpha, \gamma) \in R$ and $(\gamma, \beta) \in S$ for some $\gamma \in U$,
$(\vartheta(\alpha), \vartheta(\gamma)) \in \varphi(R)$ and $(\vartheta(\gamma), \vartheta(\beta)) \in \varphi(S)$ for some $\gamma \in U$,
$(\delta, \eta) \in \varphi(R)$ and $(\eta, \zeta) \in \varphi(S)$ for some $\eta \in V$,
$(\delta, \zeta) \in \varphi(R) \mid \varphi(S)$.

Consequently,

$$\varphi(R \mid S) = \varphi(R) \mid \varphi(S).$$

Analogous arguments show that φ preserves the operations of union, complement, and converse, and maps the identity relation on the set U to the identity relation on the set V.

If $\mathfrak{A}$ and $\mathfrak{B}$ are set relation algebras with base sets U and V respectively, and if the function φ defined in the preceding paragraph maps the set of relations in $\mathfrak{A}$ onto the set of relations in $\mathfrak{B}$, then the restriction of φ to the universe of $\mathfrak{A}$ is an isomorphism from $\mathfrak{A}$ to $\mathfrak{B}$. This type of isomorphism is called a *base isomorphism*, or more precisely, the base isomorphism from $\mathfrak{A}$ to $\mathfrak{B}$ *induced by* ϑ; and the algebras $\mathfrak{A}$ and $\mathfrak{B}$ are said to be *equivalent* or *base isomorphic* (via the isomorphism induced by ϑ). If $\mathfrak{A}$ and $\mathfrak{B}$ are the full set relation algebra on U and V respectively, then the function φ *does* map the set of relations in $\mathfrak{A}$ onto the set of relations in $\mathfrak{B}$, so in this case the algebras $\mathfrak{A}$ and $\mathfrak{B}$ *are* base isomorphic. Conclusion: two full set relation algebras on sets of the same cardinality are always isomorphic and in fact they are base isomorphic.

For another class of examples of isomorphisms between relation algebras, consider an arbitrary set U. Let $\mathfrak{Re}(U)$ be the full set relation algebra on U, and $\mathfrak{Ma}(U)$ the matrix algebra on U. The function φ that maps each relation R in $\mathfrak{Re}(U)$ to the corresponding matrix M_R

in $\mathfrak{Ma}(U)$ is a bijection from $\mathfrak{Re}(U)$ to $\mathfrak{Ma}(U)$, and φ preserves the fundamental operations, including addition and relative multiplication, by the remarks in Section 1.6. Consequently, φ is an isomorphism from $\mathfrak{Re}(U)$ to $\mathfrak{Ma}(U)$.

7.6 Atomic monomorphisms

The task of constructing an isomorphism between two relation algebras is often simplified when the algebras in question are atomic. In this case, it suffices to construct a bijection between the sets of atoms that preserves the existence of suprema and preserves the Peircean operations on atoms. The result actually holds in the broader context of Boolean algebras with completely distributive operators, so we formulate it in this broader context.

Theorem 7.11. *Let $\mathfrak{A}$ and $\mathfrak{B}$ be atomic Boolean algebras with complete operators, and φ a bijection from the set of atoms in $\mathfrak{A}$ to the set of atoms in $\mathfrak{B}$ that satisfies the following supremum property: for each set X of atoms in $\mathfrak{A}$, the supremum of X exists in $\mathfrak{A}$ if and only if the supremum of the set of atoms $\{\varphi(p) : p \in X\}$ exists in $\mathfrak{B}$. If φ preserves the Peircean operations on atoms in the sense that*

$$\begin{aligned}
&u \le p \,;\, q &&\text{if and only if} &&\varphi(u) \le \varphi(p) \,;\, \varphi(q),\\
&u \le p^{\smile} &&\text{if and only if} &&\varphi(u) \le \varphi(p)^{\smile},\\
&u \le 1' &&\text{if and only if} &&\varphi(u) \le 1',
\end{aligned}$$

for all atoms p, q, and u in $\mathfrak{A}$, then φ can be extended in a unique way to an isomorphism from $\mathfrak{A}$ to $\mathfrak{B}$. In fact, the isomorphism is just the mapping ψ defined by

$$\psi(r) = \sum\{\varphi(p) : p \in X\}$$

for every element r in $\mathfrak{A}$, where X is the set of atoms below r. Moreover, every isomorphism from $\mathfrak{A}$ to $\mathfrak{B}$ is obtainable in this fashion from a bijection of the set of atoms in $\mathfrak{A}$ to the set of atoms in $\mathfrak{B}$ that satisfies the above conditions.

Proof. Consider a bijection φ from the set U of atoms in $\mathfrak{A}$ to the set V of atoms in $\mathfrak{B}$, and suppose φ satisfies the supremum property formulated in the theorem. For every subset X of U, write

$$\varphi(X) = \{\varphi(p) : p \in X\}.$$

Every element r in $\mathfrak{A}$ is the supremum of a unique set X_r of atoms in $\mathfrak{A}$, by the assumption that $\mathfrak{A}$ is atomic; in fact, X_r is the set of all atoms below r. The supremum property implies that the supremum of the set $\varphi(X_r)$ exists in $\mathfrak{B}$. Consequently, the function ψ from $\mathfrak{A}$ to $\mathfrak{B}$ that is defined by

$$\psi(r) = \sum \varphi(X_r) = \sum\{\varphi(p) : p \in U \text{ and } p \leq r\} \tag{1}$$

for every r in $\mathfrak{A}$ is well defined.

If r and s are distinct elements in $\mathfrak{A}$, then there must be an atom that is below one of the two elements, but not the other, because $\mathfrak{A}$ is atomic. The sets of atoms X_r and X_s are therefore distinct, so the images of these sets under the bijection φ are distinct sets of atoms in $\mathfrak{B}$. Consequently, the suprema of the image sets $\varphi(X_r)$ and $\varphi(X_s)$ are distinct in $\mathfrak{B}$, so $\psi(r)$ is different from $\psi(s)$, by (1). Thus, ψ is one-to-one.

An arbitrary element t in $\mathfrak{B}$ is the supremum of the set Y of atoms in $\mathfrak{B}$ that are below t, because $\mathfrak{B}$ is atomic. Let X be the uniquely determined set of atoms in $\mathfrak{A}$ that is mapped bijectively to Y by φ. The supremum r of the set X exists in $\mathfrak{A}$, by the supremum property, and X must be the set of all atoms below r, so

$$\psi(r) = \sum \varphi(X) = \sum Y = t,$$

by (1) and the definition of X. Thus, ψ is onto.

Assume now that φ preserves the Peircean operations on atoms in the sense of the theorem. To see that ψ preserves the operations on all elements, consider arbitrary elements r and s in $\mathfrak{A}$, say

$$r = \sum X \qquad \text{and} \qquad s = \sum Y,$$

where X and Y are the sets of atoms below r and s respectively. The set of atoms below $r + s$ is just the set $Z = X \cup Y$, so

$$\begin{aligned} \psi(r+s) &= \sum\{\varphi(p) : p \in Z\} = \sum\{\varphi(p) : p \in X \cup Y\} \\ &= \sum\{\varphi(p) : p \in X\} + \sum\{\varphi(p) : p \in Y\} = \psi(r) + \psi(s), \end{aligned}$$

by the definition of ψ, the definition of the set Z, and the laws of Boolean algebra. Thus, ψ preserves addition. A bijection between

Boolean algebras that preserves addition must preserve all Boolean operations, so ψ is a Boolean isomorphism.

The argument that ψ preserves the operation $\,;\,$ is similar, but more involved. The set of atoms below $r\,;s$ is the set

$$Z = \{u \in U : u \leq p\,;q \text{ for some } p \in X, q \in Y\},$$

since

$$\begin{aligned} r\,;s &= (\textstyle\sum X)\,;(\textstyle\sum Y) \\ &= \textstyle\sum\{p\,;q : p \in X, q \in Y\} \\ &= \textstyle\sum\{\textstyle\sum\{u \in U : u \leq p\,;q\} : p \in X, q \in Y\} \\ &= \textstyle\sum\{u \in U : u \leq p\,;q \text{ for some } p \in X, q \in Y\} \\ &= \textstyle\sum Z, \end{aligned}$$

by the complete distributivity of the operation $\,;\,$ in $\mathfrak{A}$, the assumption that $\mathfrak{A}$ is atomic (so every element is the sum of the set of atoms that are below it), the laws of Boolean algebra, and the definition of the set Z. Consequently,

$$\psi(r\,;s) = \textstyle\sum\{\varphi(u) : u \in Z\}, \tag{2}$$

by the definition of ψ.

Because φ is a bijection from U to V, the assumption that

$$u \leq p\,;q \qquad \text{if and only if} \qquad \varphi(u) \leq \varphi(p)\,;\varphi(q)$$

for all atoms p, q, and u in U implies that φ must map the set of atoms below $p\,;q$ in $\mathfrak{A}$ bijectively to the set of atoms below $\varphi(p)\,;\varphi(q)$ in $\mathfrak{B}$. In other words,

$$\{\varphi(u) : u \in U \text{ and } u \leq p\,;q\} = \{v \in V : v \leq \varphi(p)\,;\varphi(q)\}. \tag{3}$$

It follows that

$$\begin{aligned} \psi(r)\,;\psi(s) &= (\textstyle\sum\{\varphi(p) : p \in X\})\,;(\textstyle\sum\{\varphi(q) : q \in Y\}) \\ &= \textstyle\sum\{\varphi(p)\,;\varphi(q) : p \in X, q \in Y\} \\ &= \textstyle\sum\{\textstyle\sum\{v \in V : v \leq \varphi(p)\,;\varphi(q)\} : p \in X, q \in Y\} \\ &= \textstyle\sum\{\textstyle\sum\{\varphi(u) : u \in U \text{ and } u \leq p\,;q\} : p \in X, q \in Y\} \\ &= \textstyle\sum\{\varphi(u) : u \in U \text{ and } u \leq p\,;q \text{ for some } p \in X, q \in Y\} \\ &= \textstyle\sum\{\varphi(u) : u \in Z\} \\ &= \psi(r\,;s), \end{aligned}$$

by the definition of ψ, the complete distributivity of the operation $\,;\,$ in $\mathfrak{B}$, the assumption that $\mathfrak{B}$ is atomic, (3), the laws of Boolean algebra, the definition of the set Z, and (2). This shows that ψ preserves the operation $\,;\,$. The proofs that ψ preserves the operation $\smile$ and maps 1' to 1' are similar. Conclusion: ψ is an isomorphism from $\mathfrak{A}$ to $\mathfrak{B}$.

To see that ψ is the unique extension isomorphism of φ, consider an arbitrary isomorphism ϑ from $\mathfrak{A}$ to $\mathfrak{B}$ that agrees with φ on the elements in U. Isomorphisms preserves all existing sums, so

$$\vartheta(r) = \sum\{\vartheta(p) : p \in X\} = \sum\{\varphi(p) : p \in X\}$$

for every r in $\mathfrak{A}$, where X is the set of atoms below r. It follows from the definition of ψ that ϑ and ψ agree on all elements r in $\mathfrak{A}$, so $\vartheta = \psi$.

Turn now to the final assertion of the theorem. Consider an arbitrary isomorphism ϑ from $\mathfrak{A}$ to $\mathfrak{B}$. Certainly, ϑ maps the set of atoms in $\mathfrak{A}$ bijectively to the set of atoms in $\mathfrak{B}$, and ϑ satisfies the supremum property and preserves the Peircean operations on atoms in the sense of the theorem, because ϑ is an isomorphism. Consequently, if φ is the restriction of ϑ to the set U, then φ is a bijection from U to V that satisfies the hypotheses of the theorem, and ϑ is the unique extension of φ. Conclusion: every isomorphism from $\mathfrak{A}$ to $\mathfrak{B}$ is the unique extension of a bijection φ satisfying the hypotheses of the theorem. □

We shall refer to the preceding theorem as the *Atomic Isomorphism Theorem*. Notice that the condition on φ regarding the existence of suprema is automatically satisfied when the algebras $\mathfrak{A}$ and $\mathfrak{B}$ are complete. In its application to relation algebras, the theorem can be strengthened somewhat.

Corollary 7.12. *Let $\mathfrak{A}$ and $\mathfrak{B}$ be complete and atomic relation algebras. If φ is a bijection from the set of atoms in $\mathfrak{A}$ to the set of atoms in $\mathfrak{B}$ that preserves relative multiplication on atoms in the sense that*

$$u \leq p\,;q \qquad \textit{if and only if} \qquad \varphi(u) \leq \varphi(p)\,;\varphi(q)$$

for all atoms p, q, and u in $\mathfrak{A}$, then φ can be extended in a unique way to an isomorphism from $\mathfrak{A}$ to $\mathfrak{B}$. In fact, the isomorphism is just the mapping ψ defined by

$$\psi(r) = \sum\{\varphi(p) : p \in X\}$$

for every r in $\mathfrak{A}$, where X is the set of atoms below r. Moreover, every isomorphism from $\mathfrak{A}$ to $\mathfrak{B}$ is obtained in this fashion from a bijection of the set of atoms in $\mathfrak{A}$ to the set of atoms in $\mathfrak{B}$ that satisfies the above condition.

Proof. Let $\mathfrak{A}'$ and $\mathfrak{B}'$ be the algebras obtained from $\mathfrak{A}$ and $\mathfrak{B}$ respectively by deleting the operation of converse and the identity element. Assume φ is a bijection from the set of atoms in $\mathfrak{A}$ to the set of atoms in $\mathfrak{B}$ that preserves relative multiplication on atoms. Apply the Atomic Isomorphism Theorem, with $\mathfrak{A}'$ and $\mathfrak{B}'$ in place of $\mathfrak{A}$ and $\mathfrak{B}$, to obtain an isomorphism ψ from $\mathfrak{A}'$ to $\mathfrak{B}'$ that extends φ. The mapping ψ is a bijection from the relation algebra $\mathfrak{A}$ to the relation algebra $\mathfrak{B}$ that preserves the operations of addition and relative multiplication. As was observed in Section 7.2, such a mapping must automatically be an isomorphism from $\mathfrak{A}$ to $\mathfrak{B}$. $\square$

As an application of the preceding corollary, consider two groups, say G and H. The atoms in the complex algebras of these groups are (the singletons of) the elements in the groups. A group isomorphism φ from G to H clearly preserves the operation of relative multiplication on atoms in the complex algebra, since

$$u = p \circ q \qquad \text{if and only if} \qquad \varphi(u) = \varphi(p) \circ \varphi(q)$$

for all elements p, q, and u in G (where $\circ$ is the operation of composition in the groups), and since relative multiplication in the complex algebras, when restricted to atoms, coincides with group composition. Apply Corollary 7.12 to conclude that the group isomorphism φ can be extended in a unique way to a relation algebra isomorphism from $\mathfrak{Cm}(G)$ to $\mathfrak{Cm}(H)$, and that every relation algebra isomorphism from $\mathfrak{Cm}(G)$ to $\mathfrak{Cm}(H)$ arises in this fashion from a corresponding group isomorphism from G to H.

Atomic Subalgebra Theorem 6.21 can be combined with the Atomic Isomorphism Theorem to arrive at a useful condition for a verifying that a given mapping from the set of atoms of an atomic relation algebra into a (not necessarily atomic) relation algebra can be extended to a complete monomorphism. As before, the result holds in the more general context of Boolean algebras with completely distributive operators.

Theorem 7.13. *Let $\mathfrak{A}$ be an atomic Boolean algebra with complete operators, U the set of atoms in $\mathfrak{A}$, and $\mathfrak{C}$ an arbitrary Boolean algebra*

with complete operators. Suppose φ is a mapping from U into $\mathfrak{C}$ with the following properties.

(i) *The elements $\varphi(p)$, for p in U, are non-zero, mutually disjoint, and sum to* 1 *in $\mathfrak{C}$.*
(ii) $1\text{'} = \sum\{\varphi(u) : u \in U \text{ and } u \leq 1\text{'}\}$.
(iii) $\varphi(p)^{\smile} = \sum\{\varphi(u) : u \in U \text{ and } u \leq p^{\smile}\}$ *for all p in U.*
(iv) $\varphi(p) \,;\, \varphi(q) = \sum\{\varphi(u) : u \in U \text{ and } u \leq p \,;\, q\}$ *for all p, q in U.*
(v) *For every subset X of U, the sum $\sum X$ exists in $\mathfrak{A}$ if and only if the sum $\sum\{\varphi(p) : p \in X\}$ exists in $\mathfrak{C}$.*

Then φ can be extended in a unique way to a complete monomorphism from $\mathfrak{A}$ into $\mathfrak{C}$. In fact, the monomorphism is just the mapping ψ defined by

$$\psi(r) = \sum\{\varphi(p) : p \in X\}$$

for every element r in $\mathfrak{A}$, where X is the set of atoms below r.

Proof. On the basis of condition (i), each of conditions (ii)–(iv) may be formulated in a somewhat different way. Condition (ii) is equivalent to the assertion that for all u in U,

$$\begin{aligned} u \leq 1\text{'} \qquad &\text{implies} \qquad \varphi(u) \leq 1\text{'}, \\ u \cdot 1\text{'} = 0 \qquad &\text{implies} \qquad \varphi(u) \cdot 1\text{'} = 0 \end{aligned}$$

(where the elements and operations on the left are those of $\mathfrak{A}$, and the ones on the right are those of $\mathfrak{B}$). Condition (iii) is equivalent to the assertion that for all u in U,

$$\begin{aligned} u \leq p^{\smile} \qquad &\text{implies} \qquad \varphi(u) \leq \varphi(p)^{\smile}, \\ u \cdot p^{\smile} = 0 \qquad &\text{implies} \qquad \varphi(u) \cdot \varphi(p)^{\smile} = 0. \end{aligned}$$

Condition (iv) is equivalent to the assertion that for all u in U,

$$\begin{aligned} u \leq p \,;\, q \qquad &\text{implies} \qquad \varphi(u) \leq \varphi(p) \,;\, \varphi(q), \\ u \cdot (p \,;\, q) = 0 \qquad &\text{implies} \qquad \varphi(u) \cdot (\varphi(p) \,;\, \varphi(q)) = 0. \end{aligned}$$

For example, to see that the last two implications are equivalent to condition (iv), suppose first that condition (iv) holds. The first implication trivially follows from (iv). To establish the second implication, suppose that u is disjoint from $p \,;\, q$. In this case, u is different from every atom v that is below $p \,;\, q$, so $\varphi(u)$ must be disjoint from $\varphi(v)$

for every such v, by the assumption in condition (i) that images of distinct atoms in U are disjoint. Consequently,

$$\begin{aligned}
0 &= \textstyle\sum\{\varphi(u)\cdot\varphi(v) : v \in U \text{ and } v \le p\,;q\} \\
&= \varphi(u)\cdot\bigl(\textstyle\sum\{\varphi(v) : v \in U \text{ and } v \le p\,;q\}\bigr) \\
&= \varphi(u)\cdot(\varphi(p)\,;\varphi(q)),
\end{aligned}$$

by the complete distributivity of multiplication over addition, and condition (iv). Thus, the last two implications hold.

To establish the reverse implication, assume that the last two implications hold. Observe that the unit in $\mathfrak{C}$ is the sum of the elements of the form $\varphi(u)$ for u in U, by condition (i). Each element u in U is either below $p\,;q$ or below its complement, because U is the set of atoms in $\mathfrak{A}$. If u is below $p\,;q$, then $\varphi(u)$ is below $\varphi(p)\,;\varphi(q)$, by the first implication. If u is below the complement of $p\,;q$, then $\varphi(u)$ is below the complement of $\varphi(p)\,;\varphi(q)$, by the second implication. Since $\varphi(p)\,;\varphi(q)$ and its complement partition the unit of $\mathfrak{C}$, it follows that $\varphi(p)\,;\varphi(q)$ must be the sum of the elements $\varphi(u)$ for $u \le p\,;q$. Therefore, condition (iv) holds.

The arguments that condition (ii) is equivalent to the first two implications, and condition (iii) is equivalent to the second two implications, are completely analogous and are left as an exercise.

The three pairs of implications (and their equivalence with the assumed conditions (ii)–(iv)) make it clear that φ preserves the Peircean operations on atoms in the sense of Atomic Isomorphism Theorem 7.11, namely

$$u \le p\,;q \qquad \text{if and only if} \qquad \varphi(u) \le \varphi(p)\,;\varphi(q), \tag{1}$$

$$u \le p^{\smile} \qquad \text{if and only if} \qquad \varphi(u) \le \varphi(p)^{\smile}, \tag{2}$$

$$u \le 1' \qquad \text{if and only if} \qquad \varphi(u) \le 1', \tag{3}$$

for all atoms p, q, and u in U. With the help of (1)–(3), we now show that the set

$$V = \varphi(U) = \{\varphi(p) : p \in U\}$$

satisfies the conditions of Atomic Subalgebra Theorem 6.21 (with V in place of W). The elements in V are mutually disjoint and sum to 1, by condition (i) above, so condition (i) in Theorem 6.21 holds. To verify condition (iv) of Theorem 6.21, suppose r and s are elements in V, and let p and q be elements in U such that $\varphi(p) = r$ and $\varphi(q) = s$. We have

$$
\begin{aligned}
r ; s = \varphi(p) ; \varphi(q) &= \sum\{\varphi(u) : u \in U \text{ and } u \leq p ; q\} \\
&= \sum\{\varphi(u) : u \in U \text{ and } \varphi(u) \leq \varphi(p) ; \varphi(q)\} \\
&= \sum\{t : t \in V \text{ and } t \leq r ; s\}
\end{aligned}
$$

by the choice of p and q, the assumed condition (iv) of this theorem, the equivalence in (1), and the definition of the set V. Thus, condition (iv) in Theorem 6.21 holds (with p and q replaced by r and s respectively). Conditions (ii) and (iii) in that theorem are verified in a completely analogous manner, using (3) and (2).

Apply Theorem 6.21 (with $\mathfrak{C}$ and V in place of $\mathfrak{A}$ and W respectively) to conclude that the set of all sums of subsets of V that exist in $\mathfrak{C}$ is the universe of a regular subalgebra $\mathfrak{B}$ of $\mathfrak{C}$ that is atomic, and whose atoms are precisely the elements in V (since every element in V is assumed to be non-zero, by condition (i) above).

The next step in the proof is to show that the mapping φ satisfies the conditions of Atomic Isomorphism Theorem 7.11. Certainly, φ maps the set U of atoms in $\mathfrak{A}$ onto the set V of atoms $\mathfrak{B}$, by the definition of the set V, and φ is one-to-one because distinct elements in U are mapped by φ to disjoint elements in V, by condition (i) in the theorem. Moreover, as we have seen in (1)–(3) above, φ preserves the Peircean operations on atoms. It remains to check that φ has the supremum property mentioned in Theorem 7.11. A subset X of U has a supremum in $\mathfrak{A}$ if and only if the image set

$$
\varphi(X) = \{\varphi(p) : p \in X\}
$$

has a supremum in $\mathfrak{C}$, by condition (v) in the theorem. If the image set $\varphi(X)$ has a supremum r in $\mathfrak{C}$, then r must belong to $\mathfrak{B}$, by the definition of $\mathfrak{B}$, and consequently r must be the supremum of $\varphi(X)$ in $\mathfrak{B}$. On the other hand, if $\varphi(X)$ has a supremum s in $\mathfrak{B}$, then s must be the supremum of $\varphi(X)$ in $\mathfrak{C}$, because $\mathfrak{B}$ is a regular subalgebra of $\mathfrak{C}$. Thus, X has a supremum in $\mathfrak{A}$ if and only if $\varphi(X)$ has a supremum in $\mathfrak{B}$.

Apply Theorem 7.11 to conclude that φ can be extended to an isomorphism ψ from $\mathfrak{A}$ to $\mathfrak{B}$ that is defined as in the theorem, and in fact ψ is the unique extension of φ to such an isomorphism. Since $\mathfrak{B}$ is a regular subalgebra of $\mathfrak{C}$, it follows from Lemma 7.9 that ψ is a complete monomorphism from $\mathfrak{A}$ into $\mathfrak{C}$. □

We shall refer to Theorem 7.13 as the *Atomic Monomorphism Theorem*. If the algebras $\mathfrak{A}$ and $\mathfrak{C}$ in the theorem are complete, then of

course condition (v) of the theorem is automatically satisfied. In this case, it may also be concluded that every complete monomorphism from $\mathfrak{A}$ into $\mathfrak{C}$ is the unique extension of a function φ satisfying the conditions of the theorem. Indeed, if ϑ is any complete monomorphism from $\mathfrak{A}$ into $\mathfrak{C}$, then the restriction of ϑ to the set U is a mapping φ that satisfies all of the hypotheses of the theorem, and consequently ϑ must be the unique extension of φ guaranteed by the theorem. We summarize this observation as a corollary.

Corollary 7.14. *Let $\mathfrak{A}$ be a complete and atomic Boolean algebra with completely distributive operators, U the set of atoms in $\mathfrak{A}$, and $\mathfrak{C}$ a complete Boolean algebra with completely distributive operators. If φ is a mapping from U into $\mathfrak{C}$ that possesses properties* (i)–(iv) *from Theorem 7.13, then φ can be extended in a unique way to a complete monomorphism from $\mathfrak{A}$ into $\mathfrak{C}$. Moreover, every complete monomorphism from $\mathfrak{A}$ into $\mathfrak{C}$ is obtainable in this fashion from a mapping of the set U into $\mathfrak{C}$ that possesses properties* (i)–(iv).

As an application of Corollary 7.14, consider the Cayley representation of a group $(G\,,\,\circ\,,\,^{-1}\,,\,e)$, that is to say, the function φ that represents the group as a group of permutations under the operations of relational composition and inverse. It is defined by

$$\varphi(f) = \{(g, g \circ f) : g \in G\}$$

for all f in G. The element $\varphi(f)$ is a permutation of the set G and therefore an element in the full set relation algebra $\mathfrak{Re}(G)$. The following properties of the Cayley representation are well-known and easy to prove. First of all, φ preserves the group operations in the sense that

$$\varphi(e) = id_G, \qquad \varphi(f^{-1}) = \varphi(f)^{-1}, \qquad \varphi(f \circ h) = \varphi(f) \,|\, \varphi(h).$$

(Here, the elements and operations on the left sides of the equations are those of the group G, while the ones on the right sides of the equations are the Peircean elements and operations of $\mathfrak{Re}(G)$.) Secondly, the binary relations $\varphi(f)$, for distinct elements f in G, are non-empty, mutually disjoint, and have the universal relation on G as their union. Thus, φ satisfies the hypotheses of Corollary 7.14, so it can be extended in a unique way to a complete monomorphism from the complex algebra $\mathfrak{Cm}(G)$ into $\mathfrak{Re}(G)$. This monomorphism is sometimes called the *Cayley representation* of the complex algebra $\mathfrak{Cm}(G)$.

7.7 Exchange Principle

Occasionally, one would like to show that a given relation algebra $\mathfrak{A}_0$ can be extended to a relation algebra $\mathfrak{A}$ possessing certain desirable properties. The actual construction, however, may not yield an extension of $\mathfrak{A}_0$, but rather something weaker, namely a relation algebra $\mathfrak{B}$ with the desired properties, and an isomorphism φ_0 from $\mathfrak{A}_0$ to a subalgebra $\mathfrak{B}_0$ of $\mathfrak{B}$. The isomorphism φ_0 shows that $\mathfrak{A}_0$ is structurally identical to $\mathfrak{B}_0$. One would therefore like to effect an "exchange", replacing $\mathfrak{B}_0$ with $\mathfrak{A}_0$ in order to obtain an extension of $\mathfrak{A}_0$ that has the desired properties. A small difficulty arises if $\mathfrak{A}_0$ contains elements that occur in $\mathfrak{B}$ in a structurally different and conflicting way. This obstacle may be overcome by first replacing the troublesome elements in $\mathfrak{B}$ with new elements that do not occur in $\mathfrak{A}_0$, and then effecting the exchange. The assertion that all of this is possible is called the *Exchange Principle.*

Theorem 7.15. *If a relation algebra $\mathfrak{A}_0$ is isomorphic to a subalgebra $\mathfrak{B}_0$ of a relation algebra $\mathfrak{B}$ via a mapping φ_0, then there is a relation algebra $\mathfrak{A}$ such that $\mathfrak{A}_0$ is a subalgebra of $\mathfrak{A}$, and $\mathfrak{A}$ is isomorphic to $\mathfrak{B}$ via a mapping that extends φ_0.*

Proof. Let B_1 be the set of elements that are in B but not in B_0. Choose any set A_1 that has the same number of elements as B_1 and that is disjoint from A_0, and let φ_1 be any bijection from A_1 to B_1 (see Figure 7.1). For instance, we might define

$$A_1 = \{(p, A_0) : p \in B_1\}, \qquad \text{and} \qquad \varphi_1((p, A_0)) = p$$

for every pair (p, A_0) in A_1. Let A be the union of the sets A_0 and A_1, and define a mapping φ from A to B by

$$\varphi(r) = \begin{cases} \varphi_0(r) & \text{if} \quad r \in A_0, \\ \varphi_1(r) & \text{if} \quad r \in A_1. \end{cases}$$

It is easily checked that φ is a bijection from A to B that extends φ_0. Turn the set A into a relation algebra $\mathfrak{A}$ by defining operations on A and a distinguished element in A that are the counterparts under φ^{-1} of the corresponding operations and the distinguished element of $\mathfrak{B}$. More precisely, define $1\text{'} = \varphi^{-1}(1\text{'})$, and if r and s are elements in A, then define

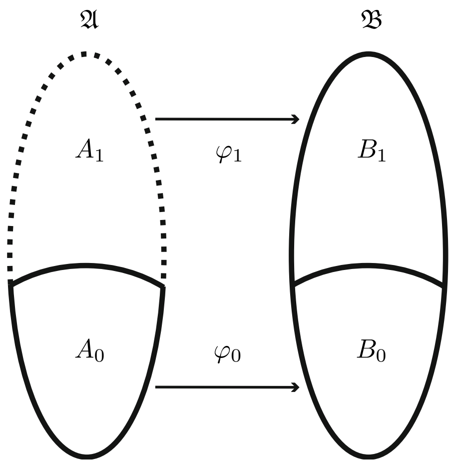


Fig. 7.1 Diagram of the Exchange Principle.

$$r + s = \varphi^{-1}(\varphi(r) + \varphi(s)), \qquad -r = \varphi^{-1}(-\varphi(r)),$$
$$r\,;s = \varphi^{-1}(\varphi(r)\,;\varphi(s)), \qquad r^{\smile} = \varphi^{-1}(\varphi(r)^{\smile}).$$

(The identity element and the operations on the right sides of the equations are those of $\mathfrak{B}$, while the ones on the left are those that are being defined for $\mathfrak{A}$.) The idea here is that to perform a certain operation on elements in A, we first translate the elements to the algebra $\mathfrak{B}$ via the mapping φ, perform the required operation on these translations in $\mathfrak{B}$, and then translate the result back to A. Under these definitions, φ automatically becomes an isomorphism from $\mathfrak{A}$ to $\mathfrak{B}$. For instance, φ preserves relative multiplication because

$$\varphi(r\,;s) = \varphi(\varphi^{-1}(\varphi(r)\,;\varphi(s))) = \varphi(r)\,;\varphi(s)$$

for any elements r and s in $\mathfrak{A}$, by the definition of relative multiplication in $\mathfrak{A}$. It follows that $\mathfrak{A}$ is the isomorphic image of $\mathfrak{B}$ under the mapping φ^{-1}, and therefore $\mathfrak{A}$ is a relation algebra with the same structural properties as $\mathfrak{B}$. Also, φ is, by definition, an extension of φ_0.

There is one more matter to check, namely that the operations of $\mathfrak{A}$, when restricted to the elements of $\mathfrak{A}_0$, coincide with the operations of $\mathfrak{A}_0$. In other words, $\mathfrak{A}_0$ should be a subalgebra of $\mathfrak{A}$. As an example, we treat the operation of relative multiplication. Let r and s be elements in $\mathfrak{A}_0$, and form their relative product in $\mathfrak{A}$. A straightforward computation shows that the result coincides with the relative product

of r and s in $\mathfrak{A}_0$:

$$\begin{aligned} r ; s = \varphi^{-1}(\varphi(r) ; \varphi(s)) = \varphi_0^{-1}(\varphi_0(r) ; \varphi_0(s)) \\ = \varphi_0^{-1}(\varphi_0(r ; s)) = r ; s. \end{aligned}$$

(The first relative product is formed in $\mathfrak{A}$, the second in $\mathfrak{B}$, the third in $\mathfrak{B}_0$, and the fourth and fifth in $\mathfrak{A}_0$.) The first equality uses the definition of relative multiplication in $\mathfrak{A}$, the second uses the fact that on elements in $\mathfrak{A}_0$, the mapping φ coincides with φ_0, the third uses the isomorphism properties of φ_0, and the last uses the fact that φ_0^{-1} is the inverse of the mapping φ_0. The other operations of $\mathfrak{A}_0$ are handled in a similar fashion. □

It should be pointed out that the Exchange Principle is really a quite general principle that applies to arbitrary algebras and structures, and not just to relation algebras.

7.8 Automorphisms

An *automorphism* of a relation algebra $\mathfrak{A}$ is an isomorphism from $\mathfrak{A}$ to $\mathfrak{A}$. Every relation algebra has at least one automorphism, namely the identity automorphism, which maps every element to itself. This is called the *trivial* automorphism. The inverse of an automorphism is again an automorphism, and the composition of two automorphisms is an automorphism, so the set of automorphisms of a relation algebra form a group under the operations of functional composition and inverse, with the identity automorphism as the group identity element.

Does every relation algebra of cardinality greater than two have a non-trivial automorphism? Somewhat surprisingly, the answer is negative. In fact, it is known that there are Boolean algebras of cardinality greater than two for which the only automorphism is the trivial one. The corresponding Boolean relation algebra is therefore an example of a relation algebra for which the only automorphism is the trivial one. If $\mathfrak{A}$ is an abelian relation algebra that is not symmetric, then the function that maps every element to its converse is an example of a non-trivial automorphism of $\mathfrak{A}$. A concrete example of such a relation algebra is $\mathfrak{Cm}(G)$, where G is an abelian group that is not a Boolean group (so not every element in G is its own inverse).

To give an example of a class of automorphisms, consider a permutation f in a relation algebra $\mathfrak{A}$, that is to say, an element f satisfying the equations

$$f^{\smile} ; f = f ; f^{\smile} = 1'$$

(see the remarks at the end of Section 5.8). Define a mapping φ on the universe of $\mathfrak{A}$ by

$$\varphi_f(r) = f ; r ; f^{\smile}$$

for every element r.

Lemma 7.16. *The function φ_f is an automorphism of $\mathfrak{A}$.*

Proof. Let $g = f^{\smile}$. Observe that the composite functions $\varphi_f \circ \varphi_g$ and $\varphi_g \circ \varphi_f$ are both the identity mapping on the universe of $\mathfrak{A}$. For instance,

$$\begin{aligned}\varphi_f(\varphi_g(r)) &= f ; (g ; r ; g^{\smile}) ; f^{\smile} = f ; (f^{\smile} ; r ; f^{\smile\smile}) ; f^{\smile} \\ &= f ; (f^{\smile} ; r ; f) ; f^{\smile} = (f ; f^{\smile}) ; r ; (f^{\smile} ; f) \\ &= 1' ; r ; 1' = r\end{aligned}$$

for every r in $\mathfrak{A}$, by the definitions of the mappings φ_f and φ_g, the definition of g, the first involution law, the associative law for relative multiplication, the definition of a permutation, and the identity law for relative multiplication. It follows that the functions φ_f and φ_g are inverses of one another, and therefore φ_f maps the set A bijectively to itself. The mapping φ_f preserves addition, by the distributive law for relative multiplication. The proof that φ_f also preserves relative multiplication reduces to a simple computation: if r and s are in $\mathfrak{A}$, then

$$\begin{aligned}\varphi_f(r ; s) = f ; r ; s ; f^{\smile} &= f ; r ; 1' ; s ; f^{\smile} \\ &= f ; r ; f^{\smile} ; f ; s ; f^{\smile} = \varphi_f(r) ; \varphi_f(s),\end{aligned}$$

by the definition of φ_f, the identity and associative laws for relative multiplication, and the definition of a permutation. Since φ_f is a bijection of the universe of $\mathfrak{A}$ that preserves addition and relative multiplication, it must be an isomorphism, and therefore an automorphism, by the remarks in Section 7.2. □

Automorphisms of the form φ_f for some permutation f in $\mathfrak{A}$ are called *inner automorphisms* of $\mathfrak{A}$. They form a subgroup of the group of all automorphisms of $\mathfrak{A}$.

7.9 Elementary embeddings

A mapping φ from $\mathfrak{A}$ to $\mathfrak{B}$ is said to be *elementary* if it preserves all properties that are expressible in the elementary (that is to say, the first-order) language $\mathcal{L}$ of relation algebras (see Section 2.4). This means that for every formula $\Gamma(v_0, \dots, v_{n-1})$ in $\mathcal{L}$, an arbitrary sequence $r = (r_0, \dots, r_{n-1})$ of elements from $\mathfrak{A}$ satisfies Γ in $\mathfrak{A}$ if and only if the image sequence

$$\varphi(r) = (\varphi(r_0), \dots, \varphi(r_{n-1}))$$

satisfies Γ in $\mathfrak{B}$. The formulas expressing that two elements are distinct, that some element is the relative product of two other elements, and so on, are all first-order, so they are satisfied by a sequence r in $\mathfrak{A}$ if and only if they are satisfied by the image sequence $\varphi(r)$ in $\mathfrak{B}$, whenever φ is elementary. From this observation, it follows at once that an elementary mapping is necessarily a monomorphism. For that reason, an elementary mapping is usually called an *elementary embedding.*

There is a characterization of elementary embeddings that is similar in flavor and in proof to the characterization in Lemma 7.9 of complete embeddings.

Lemma 7.17. *A monomorphism φ from $\mathfrak{A}$ into $\mathfrak{B}$ is elementary if and only if the image of $\mathfrak{A}$ under φ is an elementary subalgebra of $\mathfrak{B}$.*

Proof. The image of $\mathfrak{A}$ under the monomorphism φ is a subalgebra of $\mathfrak{B}$, which we denote by $\mathfrak{C}$ (see Lemma 7.4). Consider an arbitrary formula $\Gamma(v_0, \dots, v_{n-1})$ in $\mathcal{L}$ and an arbitrary sequence r of n elements in $\mathfrak{A}$. The mapping φ is an isomorphism from $\mathfrak{A}$ to $\mathfrak{C}$, so the sequence r satisfies Γ in $\mathfrak{A}$ if and only if the image sequence $\varphi(r)$ satisfies Γ in $\mathfrak{B}$, by the preservation properties of isomorphisms.

If $\mathfrak{C}$ is an elementary subalgebra of $\mathfrak{B}$, then $\varphi(r)$ satisfies Γ in $\mathfrak{C}$ if and only if it satisfies Γ in $\mathfrak{B}$, and therefore r satisfies Γ in $\mathfrak{A}$ if and only if $\varphi(r)$ satisfies Γ in $\mathfrak{B}$, by the observations of the first paragraph. Since this is true for all formulas Γ and all appropriate sequences r, it follows that φ must be an elementary embedding of $\mathfrak{A}$ into $\mathfrak{B}$.

On the other hand, if φ is an elementary embedding of $\mathfrak{A}$ into $\mathfrak{B}$, then r satisfies Γ in $\mathfrak{A}$ if and only if $\varphi(r)$ satisfies Γ in $\mathfrak{B}$, and therefore $\varphi(r)$ satisfies Γ in $\mathfrak{C}$ if and only if it satisfies Γ in $\mathfrak{B}$, by the observations of the first paragraph. Every sequence s in $\mathfrak{C}$ can be written in the form $s = \varphi(r)$ for a uniquely determined sequence r of

elements in $\mathfrak{A}$, by the definition of $\mathfrak{C}$ and the assumption that φ is a monomorphism. Consequently, an arbitrary sequence s satisfies Γ in $\mathfrak{C}$ if and only if s satisfies Γ in $\mathfrak{B}$. Since this is true for all formulas Γ and all appropriate sequences s, it follows that $\mathfrak{C}$ is an elementary subalgebra of $\mathfrak{B}$. $\square$

7.10 Historical remarks

The notion of a homomorphism is of course general algebraic in nature and was studied in various concrete algebraic contexts as early as the first decades of the 1900s. In its application to relation algebras, it was studied by Tarski in the early 1940s (as is documented in [105]). Lemmas 7.7, 7.4, and 7.6 are well-known, simple results that are applicable to arbitrary algebras.

The preservation of equations under homomorphisms on arbitrary algebras was first pointed out by Garrett Birkhoff in [12]. Lyndon [69] proved that a first-order property of algebras is preserved under homomorphisms if and only if that property can be expressed by a positive formula.

The definability of converse in terms of the other relation algebraic operations is due to Tarski [105], and first appeared in print in [23]. The fact that converse can be defined by a positive formula is an unpublished result of Tarski [112] that was inspired by Lyndon's preservation theorem in [69]. In [105], one can also find the statement that any bijection between two relation algebras which preserves addition and relative multiplication is automatically an isomorphism.

The class of examples of homomorphisms given in Section 7.3 is actually a special case of a much more general result due to Tarski [105] and published in Jónsson-Tarski [55]. The more general result will be discussed in Theorem 10.2 below.

The importance of complete monomorphisms in the context of relation algebras first came to light in the work of Lyndon (see, for example, [70]). The notion also plays an important role in the works of Maddux (see, for example, [75]) and Hirsch and Hodkinson (see, for example, [43]). Lemmas 7.9 and 7.10 apply to arbitrary Boolean algebras with or without additional operations; see [38].

The notion of an isomorphism, like that of a homomorphism, is general algebraic in nature and dates back at least to the first decades

of the 1900s. The notion of a base isomorphism was introduced by Lyndon in [70] under a different name. The terminology *base isomorphism* was introduced and extensively studied in [42] in the context of cylindric algebras.

Versions of Theorems 7.11 and 7.13 in Section 7.6 are valid for Boolean algebras with complete operators of arbitrary ranks (see Exercises 7.40 and 7.48), and also for Boolean algebras with quasi-complete operators of arbitrary ranks (see Exercises 7.41, 7.42, 7.49, and 7.50). The conditions on the operators must be replaced by conditions that apply to complete operators, or quasi-complete operators respectively, of arbitrary rank n, and not just of ranks 0, 1, and 2. The particular formulation and proof of Theorem 7.11 given here are due to Givant. In its application to complete and atomic Boolean algebras with complete operators, the theorem may be derived rather easily from two theorems that apparently date back to the work of Jónsson-Tarski [54]. The first, which is stated explicitly as Theorem 3.9 in [54], says that the complex algebra of a relational structure is always a complete and atomic Boolean algebra with complete operators (see Corollary 19.4 in Chapter 19), and every complete and atomic Boolean algebra with complete operations is isomorphic to the complex algebra of some relational structure (see Corollary 19.6). The second is not stated explicitly in [54], but may well have been known to Jónsson and Tarski (see Theorem 3.10 in [54]), and it does occur explicitly in Corollary 2.7.37 of Henkin-Monk-Tarski [41]. It says that two relational structures are isomorphic if and only if their complex algebras are isomorphic (see Corollary 19.10). Theorem 7.13 and Corollary 7.14 are due to Givant, as are the extensions of Theorems 7.11 and 7.13 to Boolean algebras with quasi-complete operators (see Exercises 7.41, 7.42, 7.49, and 7.50). The Cayley representation of a group complex algebra is much older, perhaps dating back to the 1940s. It was mentioned by Tarski in his lectures [112].

The Exchange Principle from Section 7.7 is also general algebraic in nature. The author first learned of the principle in the graduate-level lectures on abstract algebra given by Abraham Seidenberg at the University of California at Berkeley in the spring of 1967, but the principle probably dates back to the 1930s.

The examples of relation algebraic automorphisms given in Section 7.8, and in particular, Lemma 7.16, are due to Tarski and date back to [105]. The negative results in Exercises 7.21 and 7.22 are due to Andréka and Givant. The results in Exercises 7.35 and 7.45–7.46,

together with the example given after Corollary 7.12 and the result implicit in Exercise 7.56, are due to Givant. The theorem in Exercise 7.51 is due to Lyndon [70].

The notion of an elementary embedding was first introduced by Tarski and Vaught in [114], and Lemma 7.17 (formulated for arbitrary relational structures) is due to them.

Exercises

7.1. If φ is a homomorphism from $\mathfrak{A}$ into $\mathfrak{B}$, and ψ a homomorphism from $\mathfrak{B}$ into $\mathfrak{C}$, prove that the composition $\psi \circ \varphi$, defined by

$$(\psi \circ \varphi)(r) = \psi(\varphi(r))$$

for every r in $\mathfrak{A}$, is a homomorphism from $\mathfrak{A}$ into $\mathfrak{C}$. Show further that if φ and ψ are both one-to-one, or both onto, then their composition is one-to-one or onto respectively.

7.2. Prove that the inverse of an isomorphism from $\mathfrak{A}$ to $\mathfrak{B}$ is an isomorphism from $\mathfrak{B}$ to $\mathfrak{A}$.

7.3. Complete the proof in Section 7.1 that the homomorphic image of a relation algebra is again a relation algebra, by verifying that Axioms (R1)–(R6) and (R8)–(R10) are preserved under the passage to homomorphic images.

7.4. Complete the proof of Lemma 7.1 by treating the cases when γ is one of the terms $\sigma + \tau$, or $-\sigma$, or $\sigma^{\smile}$.

7.5. Complete the proof of Lemma 7.2 by treating the cases when Γ is the conjunction $\Delta \wedge \Phi$.

7.6. Prove directly, without using Lemmas 7.1 or 7.2, that the image of an equivalence element under a homomorphism must be an equivalence element. Formulate and prove the analogous results for right-ideal elements, ideal elements, subidentity elements, rectangles, functions, bijections, and permutations.

7.7. Prove directly, without using Lemma 7.2 or Corollary 7.3, that if a relation algebra $\mathfrak{A}$ is commutative, or symmetric, then every homomorphic image of $\mathfrak{A}$ is commutative or symmetric respectively.

7.8. Let φ be a homomorphism from $\mathfrak{A}$ into $\mathfrak{B}$, and $\mathfrak{C}$ a subalgebra of $\mathfrak{A}$. Prove that the restriction of φ to $\mathfrak{C}$ is a homomorphism from $\mathfrak{C}$ into $\mathfrak{B}$. If φ is one-to-one or onto, is the restriction of φ to $\mathfrak{C}$ necessarily one-to-one or onto respectively?

7.9. Suppose $(\mathfrak{A}_i : i \in I)$ and $(\mathfrak{B}_i : i \in I)$ are directed systems of relation algebras with unions $\mathfrak{A}$ and $\mathfrak{B}$ respectively. For each index i, let φ_i be a homomorphism from $\mathfrak{A}_i$ into $\mathfrak{B}_i$. The system $(\varphi_i : i \in I)$ is said to be *directed* if any two homomorphisms φ_i and φ_j in the system have a common extension to a homomorphism φ_k in the system, that is to say, φ_k agrees with φ_i on $\mathfrak{A}_i$ and with φ_j on $\mathfrak{A}_j$. If the system of homomorphisms is directed, prove that the union of the system is a homomorphism from $\mathfrak{A}$ into $\mathfrak{B}$. If the homomorphisms in the directed system are all one-to-one or all onto, prove that the union of the system is one-to-one or onto respectively.

7.10. Suppose φ is a homomorphism from $\mathfrak{A}$ into $\mathfrak{B}$. If the range of φ includes a set of generators of $\mathfrak{B}$, prove that φ is an epimorphism.

7.11. Complete the proof of Lemma 7.4 by showing that If φ is a homomorphism from $\mathfrak{A}$ into $\mathfrak{B}$, and if D is a subuniverse of $\mathfrak{B}$, prove that the inverse image set

$$\varphi^{-1}(D) = \{r \in A : \varphi(r) \in D\}$$

is a subuniverse of $\mathfrak{A}$.

7.12. Prove that a homomorphism φ on a relation algebra $\mathfrak{A}$ is one-to-one if and only if $\varphi(r) \neq 0$ for every non-zero element r in $\mathfrak{A}$.

7.13. Give an example to show that the homomorphic image of an atomless relation algebra may be atomic.

7.14. Prove that the image of an atom under an epimorphism need not be an atom. Is the image of an atom under a monomorphism necessarily an atom?

7.15. If a homomorphism maps two atoms to non-zero elements, prove that it must maps them to distinct elements.

7.16. If a homomorphism φ on an atomic relation algebra maps atoms to non-zero elements, prove that φ must in fact be a monomorphism.

7.17. Prove: a complete homomorphism from a complete and atomic relation algebra $\mathfrak{A}$ into an atomic relation algebra $\mathfrak{B}$ that maps the set of atoms in $\mathfrak{A}$ onto the set of atoms in $\mathfrak{B}$ is necessarily an isomorphism.

7.18. Use Lemma 7.1 to give an alternative proof of Lemma 7.6 (see Exercise 6.4).

7.19. Show that even for an epimorphism φ from one relation algebra to another, the inequality $\varphi(r) \leq \varphi(s)$ need not imply $r \leq s$.

7.20. Prove that a degenerate relation algebra cannot be mapped homomorphically into a non-degenerate one.

7.21. A well-known homomorphism extension theorem for Boolean algebras says that a mapping φ from a generating set X of a Boolean algebra A into a Boolean algebra B can be extended to a homomorphism from A into B if and only if

$$\prod\{p(r, \psi(r)) : r \in Y\} = 0 \quad \text{implies} \quad \prod\{p(\varphi(r), \psi(r)) : r \in Y\} = 0$$

for every finite subset Y of X, and every function ψ from Y into $\{0, 1\}$, where

$$p(r, i) = \begin{cases} \;\; r & \text{if} \quad i = 1, \\ -r & \text{if} \quad i = 0 \end{cases}$$

(see, for example, Theorem 4 on p. 107 of [38]). Prove that this theorem is not true for relation algebras.

7.22. Another well-known homomorphism extension theorem for Boolean algebras says that if A, B, and C are Boolean algebras, with A a subalgebra of B, and C complete, then any homomorphism from A into C can be extended to a complete homomorphism from B into C (see, for example, Theorem 5 on p. 114 of [38]). Prove that this theorem is not true for relation algebras.

7.23. Find a formula in the first-order language of relation algebras that defines complement in terms of addition.

7.24. Prove directly that the homomorphism φ defined in Section 7.3 preserves the operation of converse.

7.25. Find an analogue of the example in Section 7.3 for arbitrary relation algebras.

7.26. Suppose φ is a homomorphism from $\mathfrak{A}$ into $\mathfrak{B}$. If a set X of elements in $\mathfrak{A}$ has a supremum s, show that $\varphi(s)$ is an upper bound for the set $Y = \{\varphi(r) : r \in X\}$ in $\mathfrak{B}$. Conclude that if the supremum of Y exists in $\mathfrak{B}$, then that supremum must be below $\varphi(s)$.

7.27. Prove that the following condition is necessary and sufficient for a homomorphism φ from $\mathfrak{A}$ to $\mathfrak{B}$ to be complete: whenever a subset X of $\mathfrak{A}$ has the supremum 1 in $\mathfrak{A}$, the image of X under φ has the supremum 1 in $\mathfrak{B}$.

7.28. Prove that a complete homomorphism preserves all infima that happen to exist.

7.29. If a homomorphism φ between relation algebras preserves all infima that happen to exist, prove that φ must be a complete homomorphism.

7.30. Prove that the following condition is necessary and sufficient for a homomorphism φ from $\mathfrak{A}$ to $\mathfrak{B}$ to be complete: whenever a subset X of $\mathfrak{A}$ has the infimum 0 in $\mathfrak{A}$, the image of X under φ has the infimum 0 in $\mathfrak{B}$.

7.31. Suppose relation algebras $\mathfrak{A}$ and $\mathfrak{B}$ are isomorphic. Give a direct proof that $\mathfrak{A}$ is atomic, or atomless, or complete if and only if $\mathfrak{B}$ is atomic, or atomless, or complete respectively.

7.32. Suppose φ is an isomorphism from $\mathfrak{A}$ to $\mathfrak{B}$, and $\Gamma(v_0, \dots, v_{n-1})$ a formula in the language of relation algebras. Prove that a sequence $(r_0, \dots, r_{n-1})$ of elements from $\mathfrak{A}$ satisfies Γ in $\mathfrak{A}$ if and only if the image sequence $(\varphi(r_0), \dots, \varphi(r_{n-1}))$ satisfies Γ in $\mathfrak{B}$.

7.33. Prove that the complex algebra of a group, a geometry, or a lattice can never be isomorphic to the full algebra of relations on a set of cardinality at least two.

7.34. Prove that the complex algebra of a group with at least two elements cannot be isomorphic to the complex algebra of a geometry of order at least three.

7.35. Prove that the complex algebra of a Boolean group—that is to say, a group in which each element is its own inverse—is always isomorphic to the complex algebra of a projective geometry of order two. Is the converse true?

7.36. Let ϑ be a bijection from a set U to a set V, and φ the induced bijection from the set of relations on U to the set of relations on V that is defined by

$$\varphi(R) = \{(\vartheta(\alpha), \vartheta(\beta)) : (\alpha, \beta) \in R\}$$

for every relation R on U. Prove directly that φ preserves the operations of union, complement, and converse on relations, and that ϑ maps the identity relation on U to the identity relation on V.

7.37. Suppose ϑ is an arbitrary mapping (not necessarily a bijection) from a set U into a set V, and φ is the mapping from the set of relations on U into the set of relations on V that is defined as in Exercise 7.36. Which of the basic operations on relations discussed in Chapter 1 are preserved by φ? Is φ a homomorphism from $\mathfrak{Re}(U)$ into $\mathfrak{Re}(V)$? What if ϑ is one-to-one? What if ϑ is onto?

7.38. Let ϑ be an arbitrary mapping from a set U onto a set V. Define a mapping φ from the set of relations on V to the set of relations on U by

$$\varphi(R) = \{(\alpha, \beta) : (\vartheta(\alpha), \vartheta(\alpha)) \in R\}$$

for every relation R on V. Which of the basic operations on relations does φ preserve? Is φ a homomorphism?

7.39. Complete the proof of Atomic Isomorphism Theorem 7.11 by showing that the function ψ preserves the operation of converse and maps the identity element in $\mathfrak{A}$ to the identity element in $\mathfrak{B}$.

7.40. Formulate and prove a version of Atomic Isomorphism Theorem 7.11 that applies to Boolean algebras with complete operators of arbitrary ranks.

7.41. Prove the following version of Atomic Isomorphism Theorem Theorem 7.11 for Boolean algebras with quasi-complete operators. Let $\mathfrak{A}$ and $\mathfrak{B}$ be atomic Boolean algebras with quasi-complete operators of the same similarity type as relation algebras, and φ a bijection from the set of quasi-atoms in $\mathfrak{A}$ to the set of quasi-atoms in $\mathfrak{B}$ that maps zero to zero and satisfies the following supremum property: for each set X of atoms in $\mathfrak{A}$, the supremum of X exists in $\mathfrak{A}$ if and only if the supremum of the set of atoms $\{\varphi(p) : p \in X\}$ exists in $\mathfrak{B}$. If φ preserves the Peircean operations on quasi-atoms in the sense that

$$\begin{array}{lll} u \le p \,;\, q & \text{if and only if} & \varphi(u) \le \varphi(p) \,;\, \varphi(q), \\ u \le p^{\smile} & \text{if and only if} & \varphi(u) \le \varphi(p)^{\smile}, \\ u \le 1\text{'} & \text{if and only if} & \varphi(u) \le 1\text{'}, \end{array}$$

for all quasi-atoms p and q, and all atoms u, in $\mathfrak{A}$, then φ can be extended in a unique way to an isomorphism from $\mathfrak{A}$ to $\mathfrak{B}$. In fact, the isomorphism is just the mapping ψ defined by

$$\psi(r) = \sum\{\varphi(p) : p \in X\}$$

for every element r in $\mathfrak{A}$, where X is the set of atoms below r. Moreover, every isomorphism from $\mathfrak{A}$ to $\mathfrak{B}$ is obtainable in this fashion from a bijection of the set of quasi-atoms in $\mathfrak{A}$ to the set of quasi-atoms in $\mathfrak{B}$ that satisfies the above conditions.

7.42. Formulate and prove a version of Atomic Isomorphism Theorem 7.11 that applies to Boolean algebras with quasi-complete operators of arbitrary ranks.

7.43. Prove that the algebra constructed in Exercise 6.44 is isomorphic to the complex algebra of the group of integers.

7.44. Prove that the group of automorphism of a group G is isomorphic to the group of automorphisms of the complex algebra $\mathfrak{Cm}(G)$.

7.45. A *collineation* is a bijection between geometries that preserves the relation of collinearity. Prove that every collineation from a geometry P to a geometry Q can be extended in a unique way to an isomorphism from the complex algebra $\mathfrak{Cm}(P)$ to the complex algebra $\mathfrak{Cm}(Q)$; and conversely, every isomorphism from $\mathfrak{Cm}(P)$ to $\mathfrak{Cm}(Q)$ is the extension of a uniquely determined collineation from P to Q. Conclude that the group of automorphisms of $\mathfrak{Cm}(P)$ is isomorphic to the group of autocollineations of P.

7.46. Formulate and prove a version of Exercise 7.45 that applies to lattice complex algebras.

7.47. Fill in the missing details in the proof of Theorem 7.13.

7.48. Formulate and prove a version of Theorem 7.13 that applies to Boolean algebras with complete operators of arbitrary ranks.

7.49. Prove the following version of Theorem 7.13 that applies to Boolean algebras with quasi-complete operators of the same similarity type as relation algebras. Let $\mathfrak{A}$ be an atomic Boolean algebra with quasi-complete operators, U the set of atoms in $\mathfrak{A}$, and $\mathfrak{C}$ an arbitrary Boolean algebra with quasi-complete operators. Suppose φ is a mapping from $U \cup \{0\}$ into $\mathfrak{C}$ with the following properties.

(i) $\varphi(0) = 0$, and for p in U, the elements $\varphi(p)$ are non-zero, mutually disjoint, and sum to 1 in $\mathfrak{C}$.
(ii) $1' = \sum\{\varphi(u) : u \in U \text{ and } u \leq 1'\}$.
(iii) $\varphi(p)^{\smile} = \sum\{\varphi(u) : u \in U \text{ and } u \leq p^{\smile}\}$ for all p in $U \cup \{0\}$.
(iv) $\varphi(p) ; \varphi(q) = \sum\{\varphi(u) : u \in U \text{ and } u \leq p ; q\}$ for all p, q in $U \cup \{0\}$.
(v) For every subset X of U, the sum $\sum X$ exists in $\mathfrak{A}$ if and only if the sum $\sum\{\varphi(p) : p \in X\}$ exists in $\mathfrak{C}$.

Then φ can be extended in a unique way to a complete monomorphism from $\mathfrak{A}$ into $\mathfrak{C}$. In fact, the monomorphism is just the mapping ψ defined by

$$\psi(r) = \sum\{\varphi(p) : p \in X\}$$

for every element r in $\mathfrak{A}$, where X is the set of atoms below r.

7.50. Formulate and prove a version of Theorem 7.13 that applies to Boolean algebras with quasi-complete operators of arbitrary ranks.

7.51. Let P be a maximal subspace of a projective geometry Q, and D the affine geometry obtained from Q by deleting the points and lines of P. Thus, Q is the projective extension of P in which P is the geometry at infinity—that is to say, the geometry of ideal points and lines—of the affine geometry D. Define a function φ from $P^+ = P \cup \{\iota\}$ into $\mathfrak{Re}(D)$ by

$$\varphi(\iota) = \{(r, s) : r, s \in D \text{ and } r = s\},$$

and

$$\varphi(p) = \{(r, s) : r, s \in D, \text{ and } \operatorname{Col}(p, r, s)\}.$$

for p in P, where the ternary relation $\operatorname{Col}(p, r, s)$ is defined to hold for three points p, r, and s in Q if and only if the points are distinct and collinear. In other words, $\varphi(\iota)$ is the identity relation on D, and $\varphi(p)$ is the set of pairs of distinct affine points r, s such that p is the point at infinity of the line rs. Verify that φ possesses properties (i)–(v)

in Theorem 7.13. Conclude that φ can be extended to a complete monomorphism from the complex algebra $\mathfrak{Cm}(P)$ into $\mathfrak{Re}(D)$. This extension is called an *affine representation* of $\mathfrak{Cm}(P)$.

7.52. Complete the proof of Theorem 7.15 by showing first that the operations of addition, complement, and converse are preserved by the function φ defined in the proof, and second that these operations in $\mathfrak{A}_0$ are the restrictions of the corresponding operations in $\mathfrak{A}$.

7.53. Formulate and prove a version of Theorem 7.15 that applies to algebras of arbitrary similarity type.

7.54. Suppose $\mathfrak{A}$ is an abelian relation algebra that is not symmetric. Prove that the mapping $r \longmapsto r^{\smile}$ is a non-trivial automorphism of $\mathfrak{A}$.

7.55. Prove that the inner automorphisms of a relation algebra $\mathfrak{A}$ form a subgroup of the group of all automorphisms of $\mathfrak{A}$.

7.56. Is every group isomorphic to the group of automorphisms of some relation algebra?

Chapter 8
Ideals and quotients

Another way of constructing a new relation algebra from a given one $\mathfrak{A}$ is to "glue" some of the elements of $\mathfrak{A}$ together to form an algebra that is structurally similar to, but simpler than $\mathfrak{A}$. Congruence relations provide a natural way of carrying out such a gluing. The prototype for this construction is the ring of integers modulo n (for some positive integer n), which is constructed from the ring of integers by forming its quotient with respect to the relation of congruence modulo n. Each congruence relation on a relation algebra determines, and is determined by, the set of elements that are congruent to zero, so the whole construction can be simplified by replacing the congruence relation with the congruence class of zero. This leads to the study of ideals. The most natural place to begin the discussion, however, is with the basic notion of a congruence relation.

8.1 Congruences

A *congruence relation* on a relation algebra $\mathfrak{A}$, or a *congruence* for short, is an equivalence relation Θ on the universe of $\mathfrak{A}$ that preserves the operations of $\mathfrak{A}$ in the sense that whenever the pairs (r, t) and (s, u) are in Θ, then so are the pairs

$$(r + s, t + u), \qquad (r \,;\, s, t \,;\, u), \qquad (-r, -t), \qquad (r^{\smile}, t^{\smile}).$$

It is common to express the fact that a pair (r, t) is in Θ by writing

$$r \equiv t \mod \Theta$$

S. Givant, *Introduction to Relation Algebras*,
DOI 10.1007/978-3-319-65235-1_8

and saying that r *is congruent to* t *modulo* Θ. The preservation conditions can be expressed in this notation by saying that if

$$r \equiv t \mod \Theta \qquad \text{and} \qquad s \equiv u \mod \Theta,$$

then

$$r + s \equiv t + u \mod \Theta, \qquad -r \equiv -t \mod \Theta,$$
$$r \,;\, s \equiv t \,;\, u \mod \Theta, \qquad r^{\smile} \equiv t^{\smile} \mod \Theta.$$

Readers already familiar with the notion of the direct product of two algebras (to be defined in Section 11.1) may notice that the preservation conditions (together with the assumed reflexivity of Θ) just say that Θ is a subuniverse of the direct product $\mathfrak{A} \times \mathfrak{A}$. This observation implies that many of the notions and results concerning subuniverses carry over to congruences. In the next few sections, we shall give some examples of this carry over.

8.2 Properties preserved by congruences

All operations on the universe of a relation algebra $\mathfrak{A}$ that are definable by terms in the language of relation algebras must be preserved by a congruence on $\mathfrak{A}$. To prove this assertion, it suffices to observe that a congruence is a subuniverse of the direct product $\mathfrak{A} \times \mathfrak{A}$ and therefore must be closed under the operations on the product that are definable by terms. Since we have not yet discussed direct products and the properties that are preserved under them, it seems preferable to give here a proof that does not require their use.

Lemma 8.1. *If* Θ *is a congruence on a relation algebra* $\mathfrak{A}$, *then for every term* $\gamma(v_0, \dots, v_{n-1})$ *and every pair of sequences*

$$r = (r_0, \dots, r_{n-1}) \qquad \textit{and} \qquad s = (s_0, \dots, s_{n-1})$$

of elements in $\mathfrak{A}$, *if* $r_i \equiv s_i \mod \Theta$ *for* $i < n$, *then*

$$\gamma(r) \equiv \gamma(s) \mod \Theta.$$

Proof. The proof proceeds by induction on terms γ. Assume that

$$r_i \equiv s_i \mod \Theta \tag{1}$$

for $i < n$, with the intention of showing that

$$\gamma(r) \equiv \gamma(s) \mod \Theta. \tag{2}$$

There are two base cases to consider. If γ is a variable v_i, then the values of γ on r and s are r_i and s_i respectively, by the definition of the value of a term on a sequence of elements, so (2) holds by the hypothesis (1). If γ is the individual constant symbol 1', then the values of γ on r and on s are both the identity element in $\mathfrak{A}$, so that (2) holds by the assumption that the congruence Θ is reflexive.

Assume now as the induction hypothesis that

$$\sigma(v_0, \dots, v_{n-1}) \qquad \text{and} \qquad \tau(v_0, \dots, v_{n-1})$$

are terms satisfying the desired conclusion

$$\sigma(r) \equiv \sigma(s) \mod \Theta \qquad \text{and} \qquad \tau(r) \equiv \tau(s) \mod \Theta. \tag{3}$$

There are four cases to consider. If γ is the term $\sigma ; \tau$, then (3) and the definition of a congruence imply that

$$\sigma(r) ; \tau(r) \equiv \sigma(s) ; \tau(s) \mod \Theta,$$

so that (2) holds, by the definition of the value of a term on a sequence of elements. Similar arguments apply if γ is one of the terms $\sigma + \tau$, $-\sigma$, or $\sigma^{\smile}$. Invoke the principle of induction on terms to conclude that (2) holds for all terms γ. □

Concrete examples of operations that are preserved under congruences are the Boolean operations of multiplication, subtraction, and symmetric difference, and the Peircean operation of relative addition.

8.3 Generators of congruences

Every relation algebra $\mathfrak{A}$ has a largest congruence, namely the universal relation $A \times A$, and a smallest congruence, namely the identity relation id_A. Furthermore, the intersection of every system of congruences on $\mathfrak{A}$ is again a congruence on $\mathfrak{A}$, because the intersection of every system of subuniverses of the direct product $\mathfrak{A} \times \mathfrak{A}$ must again be a subuniverse of this product. (The intersection of the empty system is, by convention, the universal congruence $A \times A$.) More directly,

if Θ is the intersection of a system $(\Theta_i : i \in I)$ of congruences on $\mathfrak{A}$, then Θ is certainly an equivalence relation on the universe of $\mathfrak{A}$ (see Lemma 5.9(ii)). Moreover, if pairs (r, t) and (s, u) are in Θ, then these pairs belong to every congruence Θ_i in the system, and therefore so do the coordinatewise sum and relative product of these two pairs, and also the complement and converse of the pair (r, t). It follows that the sum and relative product of the two pairs, and the complement and converse of the first pair, belong to the intersection Θ, so Θ preserves the operations of $\mathfrak{A}$.

The observations of the preceding paragraph imply that if X is any set of ordered pairs from $\mathfrak{A}$, then the intersection Θ of the system of all those congruences on $\mathfrak{A}$ that include X as a subset is again a congruence on $\mathfrak{A}$. (There is always at least one congruence that includes X, namely $A \times A$.) The intersection Θ is the smallest congruence on $\mathfrak{A}$ that includes X. We say that Θ is the congruence *generated* by X, and X is called a *set of generators* of Θ. If Y is also a set of ordered pairs from $\mathfrak{A}$, and if X is included in Y, then the congruence generated by X is clearly included in the congruence generated by Y. In more detail, the congruence generated by Y includes the set Y and therefore also the set X, and the congruence generated by X is the smallest congruence on $\mathfrak{A}$ that includes X. A congruence is said to be *finitely generated* if it is generated by some finite subset.

The preceding definition of the congruence generated by a set X is top-down and non-constructive. There is a complication in developing a bottom-up characterization of the congruence generated by X: it is not enough to adjoin sums, complements, relative products, and converses of pairs in a step-wise fashion, as was done in Lemma 6.5 for subalgebras, because the final set must also be an equivalence relation on the universe. It is easy to ensure reflexivity by adjoining the relation id_A at the initial step, and to ensure symmetry by adjoining the pair (s, r) at any given step in which a pair (r, s) is adjoined. Ensuring transitivity, however, poses a greater problem. It is therefore best to postpone the whole discussion until we come to the topic of ideals.

8.4 Lattice of congruences

The relation of one congruence being included in another is a partial order on the set of all congruences on a relation algebra $\mathfrak{A}$, and under

this partial order, the set of congruences becomes a complete lattice. The infimum, or meet, of a system of congruences is the intersection of the system, and the supremum, or join, of the system is the congruence generated by the union of the system. The zero of the lattice is the identity congruence id_A and the unit is the universal congruence $A\times A$.

Just as in the case of subalgebras, the union of an arbitrary system of congruences on a relation algebra $\mathfrak{A}$ is, in general, not a congruence, but the union of a non-empty directed system of congruences on $\mathfrak{A}$—defined in the obvious way—is again a congruence on $\mathfrak{A}$. In particular, the union of a non-empty chain of congruences on $\mathfrak{A}$ is a congruence on $\mathfrak{A}$. If Θ is a congruence on $\mathfrak{A}$ that is generated by a set X, and if Y is a subset of X, then the congruence generated by Y—call it Θ_Y—is also included in Θ, by the remarks in the previous section. The system of congruences

$$(\Theta_Y : Y \subseteq X \text{ and } Y \text{ is finite})$$

is directed and includes the set X, so the union of this system must coincide with Θ. Thus, every congruence on $\mathfrak{A}$ is the union of a directed system of finitely generated congruences. A finitely generated congruence is always a compact element in the lattice of congruences on $\mathfrak{A}$. Consequently, the lattice of congruences on $\mathfrak{A}$ is compactly generated. The detailed proofs of all these assertions are very similar in spirit to the proofs of the corresponding results in Section 6.4 and are left as exercises.

The observations of the preceding paragraph are valid in the more general context of arbitrary abstract algebras. There are, however, properties of the congruence lattice of a relation algebra that are not generally valid. We begin with the following lemma, which says that on congruences on a relation algebra, the operation $\mid$ of relational composition is commutative.

Lemma 8.2. *If* Φ *and* Θ *are congruences on a relation algebra* $\mathfrak{A}$, *then* $\Phi \mid \Theta = \Theta \mid \Phi$.

Proof. To prove the lemma, it suffices to show that $\Phi \mid \Theta$ is included in $\Theta \mid \Phi$. The reverse inclusion then holds by symmetry. Consider a pair of elements (r, s) in the composite relation $\Phi \mid \Theta$. There must be an element t in $\mathfrak{A}$ such that (r, t) is in Φ and (t, s) in Θ, by the definition of relational composition. Observe that the pairs

$$(t \ominus s, t \ominus s) \qquad \text{and} \qquad (r \ominus t, r \ominus t)$$

(where $\ominus$ is the term-defined operation of symmetric difference) belong to the relations Φ and Θ respectively, because congruences are reflexive relations. Form the coordinatewise symmetric difference of the pairs

$$(r, t) \qquad \text{and} \qquad (t \ominus s, t \ominus s),$$

and also of the pairs

$$(r \ominus t, r \ominus t) \qquad \text{and} \qquad (t, s),$$

and use the fact that congruences preserve all term-defined operations, by Lemma 8.1, to conclude that the resulting pairs

$$(r \ominus (t \ominus s), t \ominus (t \ominus s)) \qquad \text{and} \qquad ((r \ominus t) \ominus t), (r \ominus t) \ominus s))$$

are in Φ and Θ respectively. Recall from Section 2.1 that symmetric difference is a Boolean group operation with 0 as the group identity element. Consequently,

$$t \ominus (t \ominus s) = (t \ominus t) \ominus s = 0 \ominus s = s$$

and

$$(r \ominus t) \ominus t = r \ominus (t \ominus t) = r \ominus 0 = r.$$

Write

$$u = r \ominus (t \ominus s) = (r \ominus t) \ominus s,$$

and combine all of the preceding observations to conclude that the pairs (u, s) and (r, u) are in Φ and Θ respectively. The pair (r, s) is therefore in $\Theta \,|\, \Phi$, by the definition of relational composition, so $\Phi \,|\, \Theta$ is included in $\Theta \,|\, \Phi$, as was to be shown. $\square$

We now show, with the help of the preceding lemma, that the composition of two congruences Φ and Θ in the lattice of congruences on a relation algebra $\mathfrak{A}$ is again a congruence. Observe that the composite relation $\Phi \,|\, \Theta$ is reflexive, because the relational composition of two reflexive relations is reflexive, by the identity and monotony laws for relational composition. In more detail,

$$id_A = id_A \,|\, id_A \subseteq \Phi \,|\, \Theta.$$

The composite relation is also an equivalence element, by Lemmas 8.2 and 5.9(v), so it is an equivalence relation on the universe of $\mathfrak{A}$. To

check that $\Phi \mid \Theta$ preserves the operations of $\mathfrak{A}$, consider two pairs in this relation, say (r, t) and (s, u). There must be an element p in $\mathfrak{A}$ such that (r, p) is in Φ and (p, t) in Θ, and there must also be an element q in $\mathfrak{A}$ such that (s, q) is in Φ, and (q, u) in Θ, by the definition of relational composition. Congruences preserve the operation of relative multiplication, so the pairs $(r ; s, p ; q)$ and $(p ; q, t ; u)$ are in Φ and in Θ respectively. It follows that the pair $(r ; s, t ; u)$ must be in $\Phi \mid \Theta$, by the definition of relational composition. Thus, the relation $\Phi \mid \Theta$ preserves the operation of relative multiplication. The proofs that this relation also preserves the operations of addition, complement, and converse are very similar and are left to the reader. Conclusion: $\Phi \mid \Theta$ is a congruence on $\mathfrak{A}$.

It has been shown that the lattice of congruences on $\mathfrak{A}$ is closed under the operations of relational composition and intersection. Apply Theorem 5.16 and its proof to conclude that the lattice is modular, and that its join operation is just relational composition. We summarize the results of this section in the following theorem.

Theorem 8.3. *The congruences on a relation algebra form a complete, compactly generated, modular lattice. The join of two congruences is their relational composition and the meet is their intersection.*

This theorem remains true in the more general context of abstract algebras in which a group operation is definable by means of some term. We shall see later that the lattice of congruences on a relation algebra is actually distributive.

8.5 Quotients

The *equivalence classes*, or *congruence classes*, of a congruence Θ on a relation algebra $\mathfrak{A}$ are the sets of the form

$$r/\Theta = \{s : r \equiv s \mod \Theta\}.$$

The set of all congruence classes of Θ is denoted by A/Θ. The properties of reflexivity, symmetry, and transitivity imply that

$$r/\Theta = s/\Theta \qquad \text{if and only if} \qquad r \equiv s \mod \Theta.$$

(This is a general property of equivalence relations.) In particular, two congruence classes are either equal or disjoint. The preservation properties make it possible to define operations of addition, complement,

relative multiplication, and converse on the set A/Θ in the following way:

$$(r/\Theta) + (s/\Theta) = (r + s)/\Theta, \qquad -(r/\Theta) = (-r)/\Theta,$$
$$(r/\Theta) \mathbin{;} (s/\Theta) = (r \mathbin{;} s)/\Theta, \qquad (r/\Theta)^{\smile} = (r^{\smile})/\Theta$$

for all r and s in $\mathfrak{A}$. (The operations on the right sides of the equations are those of $\mathfrak{A}$, while the ones on the left are the operations on congruence classes that are being defined.) To show that these operations are well defined, it must be checked that the definitions do not depend on the particular choices of the elements r and s. For instance, to verify that the operation $\mathbin{;}$ is well defined, suppose

$$r/\Theta = t/\Theta \qquad \text{and} \qquad s/\Theta = u/\Theta.$$

These equations imply that

$$r \equiv t \mod \Theta \qquad \text{and} \qquad s \equiv u \mod \Theta,$$

so

$$r \mathbin{;} s \equiv t \mathbin{;} u \mod \Theta,$$

by the preservation properties of Θ. In other words,

$$(r \mathbin{;} s)/\Theta = (t \mathbin{;} u)/\Theta,$$

from which it follows that

$$(r/\Theta) \mathbin{;} (s/\Theta) = (t/\Theta) \mathbin{;} (u/\Theta),$$

by the definition of the relative product of two congruence classes. Conclusion: in the definition of the relative product of two congruence classes, it does not matter whether r or t is used as a representative of the first congruence class, nor does it matter whether s or u is used as a representative of the second congruence class; all choices of representatives lead to the same result. The same is true of the other operations defined above.

The algebra consisting of the set of congruence classes of Θ under the four operations on congruence classes that were just defined, and with the congruence class $1'/\Theta$ as the distinguished constant, is called the *quotient of* $\mathfrak{A}$ *modulo* Θ and is denoted by $\mathfrak{A}/\Theta$. It is not difficult to show that this quotient is a relation algebra, by checking directly

the validity of the relation algebraic axioms. For example, here is the verification of Axiom (R4):

$$\begin{aligned}(r/\Theta)\,;((s/\Theta)\,;(t/\Theta)) &= (r/\Theta)\,;((s\,;t)/\Theta) = (r\,;(s\,;t))/\Theta \\ &= ((r\,;s)\,;t)/\Theta = ((r\,;s)/\Theta)\,;(t/\Theta) = ((r/\Theta)\,;(s/\Theta))\,;(t/\Theta)\end{aligned}$$

for all r, s, and t in $\mathfrak{A}$, by the definition of the operation $;$ in $\mathfrak{A}/\Theta$ and the validity of the associative law in $\mathfrak{A}$.

There is a more efficient way of proving that a quotient of a relation algebra $\mathfrak{A}$ is always a relation algebra. For a given congruence Θ on $\mathfrak{A}$, define a mapping φ from $\mathfrak{A}$ to $\mathfrak{A}/\Theta$ by writing

$$\varphi(r) = r/\Theta$$

for all r in $\mathfrak{A}$. Simple computations show that φ satisfies the conditions for being an epimorphism. For example, φ preserves the operation of relative multiplication because

$$\varphi(r\,;s) = (r\,;s)/\Theta = (r/\Theta)\,;(s/\Theta) = \varphi(r)\,;\varphi(s),$$

by the definition of φ and the definition of relative multiplication in the quotient. The remaining computations needed to show that φ is an epimorphism are left as an exercise.

Lemma 8.4. *For every congruence Θ on a relation algebra $\mathfrak{A}$, the function mapping r to r/Θ for each r in $\mathfrak{A}$ is an epimorphism from $\mathfrak{A}$ to $\mathfrak{A}/\Theta$.*

The mapping in the lemma is called the *canonical homomorphism* or the *quotient homomorphism* (or *quotient mapping*), from $\mathfrak{A}$ to $\mathfrak{A}/\Theta$. It follows from the lemma that the quotient $\mathfrak{A}/\Theta$ is a homomorphic image of $\mathfrak{A}$. Every homomorphic image of a relation algebra is again a relation algebra, by Corollary 7.3, so in particular, every quotient of a relation algebra is again a relation algebra, by Lemma 8.4. Similar arguments show that if a relation algebra is commutative or symmetric, then each of its quotients is commutative or symmetric respectively.

The observations in the preceding lemma suggest a close connection between homomorphisms and congruences. To pursue this connection further, consider an arbitrary homomorphism φ from a relation algebra $\mathfrak{A}$ into a relation algebra $\mathfrak{B}$. Define a binary relation Θ on the universe of $\mathfrak{A}$ by specifying that two elements r and s are equivalent modulo Θ just in case $\varphi(r) = \varphi(s)$. It is easy to check that Θ is a

congruence on $\mathfrak{A}$. For instance, if r and t are congruent modulo Θ, and also s and u, then

$$\varphi(r) = \varphi(t) \qquad \text{and} \qquad \varphi(s) = \varphi(u),$$

by the definition of Θ. The homomorphism properties of φ imply that

$$\varphi(r\,;s) = \varphi(r)\,;\varphi(s) = \varphi(t)\,;\varphi(u) = \varphi(t\,;u),$$

so the relative products $r\,;s$ and $t\,;u$ are also congruent modulo Θ. Consequently, Θ preserves the operation of relative multiplication. The verifications of the other congruence properties for Θ are equally easy to prove and are left as an exercise. We shall refer to Θ as the *congruence induced by* φ. (The term *kernel* of φ is sometimes employed, but we shall reserve this term for another purpose.)

Start with a congruence Θ on $\mathfrak{A}$, take φ to be the quotient homomorphism from $\mathfrak{A}$ to $\mathfrak{A}/\Theta$, and let Φ be the congruence on $\mathfrak{A}$ induced by φ. Using the definition of Φ and the definition of φ, we obtain

$$\begin{aligned} r \equiv s \mod \Phi \qquad &\text{if and only if} \qquad \varphi(r) = \varphi(s), \\ &\text{if and only if} \qquad r/\Theta = s/\Theta, \\ &\text{if and only if} \qquad r \equiv s \mod \Theta. \end{aligned}$$

Consequently, Θ coincides with Φ. This proves the following result, known as the *Homomorphism Theorem* (for congruences).

Theorem 8.5. *Every congruence* Θ *on a relation algebra* $\mathfrak{A}$ *is induced by some epimorphism*, *namely the canonical homomorphism of* $\mathfrak{A}$ *onto the quotient* $\mathfrak{A}/\Theta$.

What do the homomorphic images of a relation algebra $\mathfrak{A}$ look like? Lemma 8.4 tells us that every quotient of $\mathfrak{A}$ is a homomorphic image of $\mathfrak{A}$. The next theorem says that, up to isomorphism, these quotients are the only homomorphic images of $\mathfrak{A}$. The result is usually called the *First Isomorphism Theorem* (for congruences).

Theorem 8.6. *Every homomorphic image of a relation algebra* $\mathfrak{A}$ *is isomorphic to a quotient of* $\mathfrak{A}$ *modulo some congruence* Θ. *In fact, if* φ *is an epimorphism from* $\mathfrak{A}$ *to* $\mathfrak{B}$, *and if* Θ *is the congruence induced by* φ, *then* $\mathfrak{A}/\Theta$ *is isomorphic to* $\mathfrak{B}$ *via the function that maps* r/Θ *to* $\varphi(r)$ *for every element* r *in* $\mathfrak{A}$.

Proof. Consider an epimorphism φ from $\mathfrak{A}$ to $\mathfrak{B}$, and let Θ be the congruence on $\mathfrak{A}$ induced by φ. Use the definition of Θ to obtain the equivalences

$$\begin{aligned} \varphi(r) = \varphi(t) \qquad &\text{if and only if} \qquad r \equiv t \mod \Theta, \\ &\text{if and only if} \qquad r/\Theta = t/\Theta. \end{aligned}$$

The equivalence of the first and last equations, and the assumption that φ maps $\mathfrak{A}$ onto $\mathfrak{B}$, imply that the correspondence ψ defined by

$$\psi(r/\Theta) = \varphi(r)$$

for each element r in $\mathfrak{A}$ is a well-defined bijection from the universe of $\mathfrak{A}/\Theta$ to the universe of $\mathfrak{B}$. It is easy to check that this bijection is actually an isomorphism. For example, here is the verification that ψ preserves relative multiplication:

$$\begin{aligned} \psi((r/\Theta)\,;(s/\Theta)) = \psi((r\,;s)/\Theta) &= \varphi(r\,;s) \\ &= \varphi(r)\,;\varphi(s) = \psi(r/\Theta)\,;\psi(s/\Theta), \end{aligned}$$

by the definition of relative multiplication in $\mathfrak{A}/\Theta$, the definition of ψ, and the homomorphism properties of φ. The proof that ψ preserves addition is similar and is left to the reader. Every bijection between relation algebras that preserves addition and relative multiplication is necessarily an isomorphism, by the remarks preceding Lemma 7.7, so ψ must be an isomorphism. □

The preceding theorem is valid in the more general context of arbitrary abstract algebras. For a concrete instance of the theorem, take $\mathfrak{A}$ to be a set relation algebra in which the unit equivalence relation E has more than one equivalence class, take V to be one of the equivalence classes of E, and let φ be the homomorphism from $\mathfrak{A}$ into $\mathfrak{Re}(V)$ that is defined by $\varphi(R) = R \cap (V \times V)$ for each R in $\mathfrak{A}$ (see the examples in Section 7.3). The congruence on $\mathfrak{A}$ induced by φ is the relation Θ defined by

$$R \equiv S \mod \Theta \qquad \text{if and only if} \qquad R \cap (V \times V) = S \cap (V \times V).$$

If $\mathfrak{B}$ is the image of $\mathfrak{A}$ under the homomorphism φ, then $\mathfrak{B}$ is isomorphic to $\mathfrak{A}/\Theta$ via the function that maps R/Θ to $R \cap (V \times V)$ for each R in $\mathfrak{A}$, by the First Isomorphism Theorem.

8.6 Ideals

A congruence Θ obviously determines each of its congruence classes, and in particular it determines the congruence class of 0, which is called the *kernel* of Θ. It is a happy state of affairs that, conversely, Θ is completely determined by its kernel via the equivalence

$$r \equiv s \mod \Theta \qquad \text{if and only if} \qquad r \ominus s \equiv 0 \mod \Theta.$$

In other words, to check whether two elements r and s are congruent modulo Θ, it is necessary and sufficient to check whether their symmetric difference $r \ominus s$ is in the kernel. For the proof, suppose first that r and s are congruent modulo Θ. The element s is congruent to itself modulo Θ, because congruences are reflexive. Consequently, the elements $r \ominus s$ and $s \ominus s$ are congruent, because congruences preserve the operation of symmetric difference. The element $s \ominus s$ is equal to 0, so $r \ominus s$ is congruent to 0 and is therefore in the kernel of Θ, by the definition of the kernel. To prove the converse, suppose $r \ominus s$ is in the kernel of Θ, so that $r \ominus s$ and 0 are congruent modulo Θ. Of course s is congruent to itself, so $r \ominus s \ominus s$ is congruent to $0 \ominus s$, by the preservation properties of Θ. The first element is r and the second is s, so r is congruent to s modulo Θ.

Under what conditions is a subset of the universe of $\mathfrak{A}$ the kernel of some congruence on $\mathfrak{A}$? Clearly, arbitrary subsets cannot be kernels, because the kernel of a congruence Θ has a number of special properties that are not shared by arbitrary subsets. First of all, $0 \equiv 0 \mod \Theta$, so the element 0 must be in the kernel of Θ. Second, if $r \equiv 0 \mod \Theta$ and $s \equiv 0 \mod \Theta$, then

$$r + s \equiv 0 \mod \Theta, \qquad r \mathbin{+\!\!\!\!,} s \equiv 0 \mod \Theta, \qquad r^{\smile} \equiv 0 \mod \Theta,$$

by Boolean algebra and Lemmas 4.7(ix), 4.1(vi), and 8.1. Thus, the kernel of Θ must be closed under the operations of addition, relative addition, and converse. Third, if $r \equiv 0 \mod \Theta$, and if s is any element in $\mathfrak{A}$, then

$$r \,;\, s \equiv 0 \mod \Theta, \qquad s \,;\, r \equiv 0 \mod \Theta, \qquad r \cdot s \equiv 0 \mod \Theta,$$

by Boolean algebra, Corollary 4.17 and its first dual, and Lemma 8.1. Thus, the kernel is closed under the operations of multiplication and relative multiplication by arbitrary elements from $\mathfrak{A}$ (and not just by

elements from the kernel). It turns out that a subcollection of these properties is enough to characterize the sets that are kernels of some congruence; the remaining properties are derivable from this subcollection.

Definition 8.7. An *ideal* in a relation algebra $\mathfrak{A}$ is a subset M of the universe with the following properties.

(i) 0 is in M.
(ii) If r and s are in M, then $r + s$ is in M.
(iii) If r is in M and s in $\mathfrak{A}$, then $r \cdot s$ is in M.
(iv) If r is in M and s in $\mathfrak{A}$, then $r\,;s$ and $s\,;r$ are in M. □

These conditions are similar to the closure conditions that are satisfied by a subalgebra. (We shall derive the corresponding closure conditions for converse and relative addition in the next lemma and in Corollary 8.10 below.) Note, however, that conditions (iii) and (iv) are stronger than the corresponding subalgebra closure conditions; they say that M is closed under multiplication and relative multiplication by arbitrary elements from $\mathfrak{A}$, and not just by elements from M. Also, the closure of M under the operation of complement is not required, and is not true (except in one trivial case). Conditions (i)–(iii) are exactly the conditions that M be a *Boolean ideal* (see, for example, [38]). Thus, a relation algebraic ideal is a Boolean ideal that is closed under relative multiplication by arbitrary elements from the relation algebra. In other words, it is a Boolean ideal that satisfies condition (iv).

Each of the conditions in Definition 8.7 has a useful equivalent formulation.

Lemma 8.8. *Condition* (iii) *is equivalent to the condition*:

(v) *If r is in M and $s \leq r$, then s is in M.*

Under the assumption of condition (iii), *the following further equivalences hold. Condition* (i) *is equivalent to the condition*:

(vi) *M is not empty.*

Condition (ii) *is equivalent to the condition*:

(vii) *If r and s are in M, then $r \ominus s$ is in M.*

Condition (iv) *is equivalent to the conjunction of the two conditions*:

(viii) *If r is in M, then $r^{\smile}$ is in M.*
(ix) *If r is in M and s in $\mathfrak{A}$, then $r\,;s$ is in M.*

Proof. Suppose first that condition (iii) holds. If r is in M and $s \le r$, then the product $r \cdot s$ must be in M, by (iii). This product coincides with s, so s is in M and therefore condition (v) holds. Assume now that condition (v) holds. If r is in M and s in $\mathfrak{A}$, then $r \cdot s$ must belong to M, by (v), because $r \cdot s \le r$. Thus, condition (iii) holds.

For the remainder of the proof, we assume condition (iii) and hence also condition (v). Condition (i) obviously implies condition (vi), and the reverse implication is a direct consequence of condition (v) and the fact that 0 is below every element.

To establish the next equivalence, assume first that condition (ii) holds. If r and s are in M, then the products $r \cdot -s$ and $s \cdot -r$ are in M, by (iii), and therefore the sum of these two products is in M, by (ii). Since

$$r \ominus s = (r \cdot -s) + (s \cdot -r),$$

the validity of condition (vii) follows. Assume now that condition (vii) holds. If r and s are in M, then the product $r \cdot s$ is in M, by (iii), and therefore $r \ominus s \ominus (r \cdot s)$ is in M, by two applications of (vii). Since

$$r + s = r \ominus s \ominus (r \cdot s),$$

the validity of condition (ii) follows.

To establish the final equivalence of the lemma, assume first that condition (iv) holds. Clearly, we have condition (ix), because this condition is just one half of (iv). To obtain condition (viii), consider an arbitrary element r in M. The product $1 ; r ; 1$ belongs to M, by (iv), and $r^{\smile} \le 1 ; r ; 1$, by Corollary 5.42, so $r^{\smile}$ is in M, by (v). Thus, we obtain condition (viii). Assume now that conditions (viii) and (ix) are both valid. If r is in M, and s in $\mathfrak{A}$, then $r^{\smile}$ is in M, by (viii), and therefore $r^{\smile} ; s^{\smile}$ is in M, by (ix). Apply (viii) once more to obtain that $(r^{\smile} ; s^{\smile})^{\smile}$ is in M. Since

$$(r^{\smile} ; s^{\smile})^{\smile} = s ; r,$$

by the involution laws, we arrive at the second half of condition (iv); the first half of (iv) is just condition (ix). $\square$

We have seen that the kernel of every congruence is an ideal. The converse is also true: every ideal uniquely determines a congruence of which it is the kernel.

Theorem 8.9. *If M is an ideal in a relation algebra, and if Θ is the relation on the universe of $\mathfrak{A}$ that is defined by*

$$r \equiv s \mod \Theta \qquad \textit{if and only if} \qquad r \ominus s \in M,$$

then Θ *is a congruence on* $\mathfrak{A}$, *and* M *is the kernel of* Θ. *Moreover*, Θ *is the only congruence on* $\mathfrak{A}$ *with kernel* M.

Proof. For each element r in $\mathfrak{A}$, we clearly have $r \ominus r = 0$. Since 0 is in M, by condition (i) in the definition of an ideal, it follows from the definition of Θ that

$$r \equiv r \mod \Theta.$$

Consequently, Θ is reflexive. The symmetry of Θ is established in a similar way, using the commutative law $r \ominus s = s \ominus r$. To establish the transitivity of Θ, assume that

$$r \equiv s \mod \Theta \qquad \text{and} \qquad s \equiv t \mod \Theta.$$

The elements $r \ominus s$ and $s \ominus t$ are then both in M, by the definition of Θ, and therefore so is the symmetric difference of these two elements, by condition (vii) in Lemma 8.8. Since

$$r \ominus t = r \ominus 0 \ominus t = r \ominus (s \ominus s) \ominus t = (r \ominus s) \ominus (s \ominus t),$$

by the associative and identity laws for symmetric difference, it follows that $r \ominus t$ is in M, and consequently that $r \equiv t \mod \Theta$.

In order to verify the preservation conditions, assume

$$r \equiv t \mod \Theta \qquad \text{and} \qquad s \equiv u \mod \Theta. \tag{1}$$

The elements $r \ominus t$ and $s \ominus u$ are then in M, by the definition of Θ, and therefore the differences

$$r - t, \quad t - r, \quad s - u, \quad u - s \quad \text{are in} \quad M, \tag{2}$$

by condition (v) in Lemma 8.8 and the definition of symmetric difference. Condition (ii) in the definition of an ideal therefore implies that the sum $(r - t) + (s - u)$ is in M. Since

$$\begin{aligned}(r + s) - (t + u) &= (r + s) \cdot -t \cdot -u = r \cdot -t \cdot -u + s \cdot -t \cdot -u \\ &\le r \cdot -t + s \cdot -u = (r - t) + (s - u),\end{aligned}$$

it follows from condition (v) and the preceding observations that the difference $(r + s) - (t + u)$ is in M. A similar argument shows that the

difference $(t+u)-(r+s)$ is in M. Apply condition (ii) to conclude that the sum

$$[(r+s)-(t+u)]+[(t+u)-(r+s)]$$

is in M. This sum is just the symmetric difference $(r+s)\ominus(t+u)$, so this symmetric difference is in M, and therefore

$$r+s\equiv t+u \mod \Theta,$$

by the definition of Θ. In other words, Θ preserves addition.

The proof that Θ preserves the operations of complement and converse uses the laws

$$-r\ominus -t=r\ominus t \qquad \text{and} \qquad (r\ominus t)^{\smile}=r^{\smile}\ominus t^{\smile}.$$

(The first law is an easy consequence of the definition of symmetric difference, and the second law is Lemma 4.1(iv).) In more detail, assume that the first congruence in (1) holds. The element $r\ominus t$ is then in M, by the definition of Θ, and therefore $(r\ominus t)^{\smile}$ is in M, by condition (viii) in Lemma 8.8. The two cited laws now imply that $-r\ominus -t$ and $r^{\smile}\ominus t^{\smile}$ are in M, so

$$-r\equiv -t \mod \Theta \qquad \text{and} \qquad r^{\smile}\equiv t^{\smile} \mod \Theta,$$

by the definition of Θ.

The argument that Θ preserves relative multiplication is somewhat more involved. Assume that the congruences in (1) hold. From (2) and condition (iv) in the definition of an ideal, we obtain that the products

$$(r-t)\,;s \qquad \text{and} \qquad t\,;(s-u)$$

are both in M, and therefore so is the sum of these products, by condition (ii). Now,

$$(r\,;s)-(t\,;u)\leq[(r\,;s)-(t\,;s)]+[(t\,;s)-(t\,;u)],$$

by Boolean algebra, and

$$(r\,;s)-(t\,;s)\leq(r-t)\,;s \qquad \text{and} \qquad (t\,;s)-(t\,;u)\leq t\,;(s-u),$$

by the semi-distributive law for relative multiplication over subtraction (Lemma 4.6). Combine these inequalities to arrive at

$$(r\,;s) - (t\,;u) \leq (r-t)\,;s + t\,;(s-u).$$

As has already been observed, the sum on the right side of this inequality is in M, so the difference on the left must also be in M, by condition (v). A completely symmetric argument shows that the difference $(t\,;u)-(r\,;s)$ is in M. Consequently, the sum of these differences,

$$[(r\,;s)-(t\,;u)] + [(t\,;u)-(r\,;s)],$$

is in M, by condition (ii). Since this sum is just the symmetric difference $(r\,;s) \ominus (t\,;u)$, we arrive at the conclusion that

$$r\,;s \equiv t\,;u \mod \Theta,$$

by the definition of Θ. This completes the proof that Θ is a congruence on $\mathfrak{A}$.

The kernel of Θ is, by definition, the set of elements that are congruent to 0. In other words, it is the set of elements r such that $r \ominus 0$ belongs to M. This set is of course just M, since $r \ominus 0 = r$, so the kernel of Θ is M.

If Φ is any congruence with kernel M, then

$$\begin{aligned} r \equiv s \mod \Phi \qquad &\text{if and only if} \qquad r \ominus s \equiv 0 \mod \Phi, \\ &\text{if and only if} \qquad r \ominus s \in M, \\ &\text{if and only if} \qquad r \ominus s \equiv 0 \mod \Theta, \\ &\text{if and only if} \qquad r \equiv s \mod \Theta, \end{aligned}$$

by the remarks at the beginning of this section and the assumption that Φ and Θ both have kernel M. Thus, $\Phi = \Theta$. Conclusion: Θ is the unique congruence with kernel M. □

A consequence of the preceding theorem is the observation that an ideal is also closed under relative addition.

Corollary 8.10. *If r and s are elements in an ideal M, then $r \mathbin{+\!\!\!,} s$ is in M.*

Proof. Suppose Θ is the congruence determined by the ideal M. If r and s are in M, then

$$r \equiv 0 \mod \Theta \qquad \text{and} \qquad s \equiv 0 \mod \Theta,$$

since M is the kernel of Θ, and therefore

$$r \mathbin{+\!\!,} s \equiv 0 \mathbin{+\!\!,} 0 \mod \Theta,$$

by Lemma 8.1. The relative sum $0 \mathbin{+\!\!,} 0$ is 0, by Lemma 4.7(ix), so $r \mathbin{+\!\!,} s$ belongs to the kernel of Θ, which is M. □

All of the congruence classes of a congruence Θ can be computed directly from the kernel M of the congruence. In fact, for each element r, the congruence class r/Θ coincides with the *coset*

$$r \ominus M = \{r \ominus s : s \in M\}.$$

To prove this assertion, we check that the sets r/Θ and $r \ominus M$ have the same elements:

$$\begin{aligned} s \in r/\Theta \qquad &\text{if and only if} \qquad r \equiv s \mod \Theta, \\ &\text{if and only if} \qquad r \ominus s \in M, \\ &\text{if and only if} \qquad s \in r \ominus M. \end{aligned}$$

The first equivalence uses the definition of r/Θ, and the second uses the definition of Θ in terms of M. To prove the third equivalence, observe that if $r \ominus s$ is in M and if $t = r \ominus s$, then the element $r \ominus t$ belongs to the coset $r \ominus M$, by the definition of this coset; since

$$r \ominus t = r \ominus (r \ominus s) = (r \ominus r) \ominus s = 0 \ominus s = s,$$

it follows that s is in $r \ominus M$. On the other hand, if s belongs to the coset $r \ominus M$, then $s = r \ominus t$ for some element t in M; since $r \ominus s = t$, by a computation similar to the preceding one, it follows that $r \ominus s$ is in M.

The universe of the quotient $\mathfrak{A}/\Theta$ is defined to be the set of congruences classes of Θ, but an equivalent definition is that the universe consists of the cosets of M, where M is the kernel of Θ. Similarly, the operations of the quotient algebra are defined in terms of the congruence classes of Θ, but they can also be equivalently defined entirely in terms of the cosets of M, in the following manner:

$$\begin{aligned} (r \ominus M) + (s \ominus M) &= (r + s) \ominus M, \qquad & -(r \ominus M) &= (-r) \ominus M, \\ (r \ominus M) \,;\, (s \ominus M) &= (r \,;\, s) \ominus M, \qquad & (r \ominus M)^{\smile} &= (r^{\smile}) \ominus M. \end{aligned}$$

(The occurrences of addition, complement, relative multiplication, and converse on the left sides of these equations denote operations of $\mathfrak{A}/\Theta$,

while the ones on the right denote operations of $\mathfrak{A}$.) The zero, unit, diversity element, and identity element of the quotient algebra are

$$0 \ominus M, \qquad 1 \ominus M, \qquad 0\text{'} \ominus M, \qquad 1\text{'} \ominus M$$

respectively. (Of course, $0 \ominus M$ coincides with M.)

The fact that the definitions of the elements and operations of the quotient algebra $\mathfrak{A}/\Theta$ can be formulated entirely in terms of the cosets of the ideal M suggests the idea of dispensing with the congruence Θ, and phrasing everything in terms of the ideal M. In order to adopt a notation and terminology that is consistent with this idea, we must replace the congruence Θ everywhere with the ideal M. Thus, for example, we write r/M instead of r/Θ to denote the congruence class of an element r, and we observe that $r/M = r \ominus M$. In a similar fashion, we write $r \equiv s \mod M$ instead of $r \equiv s \mod \Theta$ to express that the elements r and s are congruent. It is easy to check that

$$r \equiv s \mod M \qquad \text{if and only if} \qquad r \ominus s \in M,$$

or, put a slightly different way,

$$r/M = s/M \qquad \text{if and only if} \qquad r \ominus s \in M.$$

Finally, we write A/M for the universe of the quotient algebra, and $\mathfrak{A}/M$ for the quotient algebra itself. We call this quotient the *quotient of* $\mathfrak{A}$ *modulo* M.

The quotient homomorphism that maps each element in $\mathfrak{A}$ to its congruence class modulo Θ can also be defined entirely in terms of cosets: it is the function φ from $\mathfrak{A}$ to $\mathfrak{A}/M$ that is determined by

$$\varphi(r) = r/M$$

for each r in $\mathfrak{A}$. The *kernel* of φ is, by definition, the set of elements that are mapped to the zero element $0/M$ of the quotient, and of course this kernel is just the ideal M.

Sets of elements (in this case, ideals) are almost always easier to deal with than sets of pairs of elements (in this case, congruences), so in the study of relation algebras, congruences are usually dispensed with, in favor of ideals. We shall follow this practice. The following lemma provides an example. It says that the property of being an ideal is preserved under epimorphisms and under inverse homomorphisms.

Lemma 8.11. *Let φ be a homomorphism from a relation algebra $\mathfrak{A}$ into a relation algebra $\mathfrak{B}$. If N is an ideal in $\mathfrak{B}$, then the inverse image set*

$$\varphi^{-1}(N) = \{r \in A : \varphi(r) \in N\}$$

is an ideal in $\mathfrak{A}$. Similarly, if M is an ideal in $\mathfrak{A}$, and if φ maps $\mathfrak{A}$ onto $\mathfrak{B}$, then the image set

$$\varphi(M) = \{\varphi(r) : r \in M\}$$

is an ideal in $\mathfrak{B}$.

Proof. The proof of the lemma is similar in spirit to the proof of Lemma 7.4. We focus on the proof of the second assertion. It must be shown that conditions (i)–(iv) in the definition of an ideal are satisfied by the image set $\varphi(M)$ in $\mathfrak{B}$. The zero element in $\mathfrak{B}$ certainly belongs to this image set, because $\varphi(0) = 0$. Thus, condition (i) holds.

To verify conditions (iii) and (iv), consider elements u in $\varphi(M)$ and v in $\mathfrak{B}$. There must be elements r in M and s in $\mathfrak{A}$ that are mapped to u and v respectively, by the definition of the image set $\varphi(M)$ and the assumption that φ is onto. The elements

$$r \cdot s, \qquad r \,;\, s, \qquad s \,;\, r,$$

all belong to M, by the assumption that M is an ideal, so the images of these elements under φ all belong to $\varphi(M)$. The homomorphism properties of φ imply that these images are just the elements

$$u \cdot v, \qquad u \,;\, v, \qquad v \,;\, u,$$

respectively, so these image elements are all in the image set $\varphi(M)$. Thus, the image set satisfies conditions (iii) and (iv) (with u and v in place of r and s respectively). A similar argument shows that $\varphi(M)$ satisfies condition (ii). Conclusion: $\varphi(M)$ is an ideal in $\mathfrak{B}$. □

8.7 Generators of ideals

Every relation algebra $\mathfrak{A}$ has a smallest ideal, namely the set $\{0\}$. This is called the *trivial ideal*; all other ideals are called *non-trivial.* Every

relation algebra $\mathfrak{A}$ also has a largest ideal, namely the universe A. This is called the *improper ideal*; all other ideals are called *proper*. Observe that an ideal is proper if and only if it does not contain the unit 1. (This follows from condition (v) in Lemma 8.8.)

The intersection of every system of ideals in a relation algebra $\mathfrak{A}$ is again an ideal. The proof consists in verifying that the conditions of Definition 8.7 hold in the intersection. For instance, to verify condition (iv), consider an element r in the intersection, and let s be any element in $\mathfrak{A}$. Every ideal in the system contains r, and therefore also contains the relative products $r\,;s$ and $s\,;r$, by condition (iv) applied to each ideal in the system. It follows that these relative products belong to the intersection of the system, so the intersection satisfies condition (iv). The other three conditions are verified in an analogous fashion.

The special case when a system of ideals is empty is worth discussing for a moment, if only to avoid later confusion. The improper ideal A is vacuously included in every ideal in the empty system (there is no ideal in the empty system that does not include A). Clearly, A is the largest ideal that is included in every ideal in the empty system, so it is, by definition, the infimum of that system. Similarly, the trivial ideal $\{0\}$ vacuously includes every ideal in the empty system (there is no ideal in the empty system that is not included in $\{0\}$). Since $\{0\}$ is obviously the smallest ideal that includes every ideal in the empty system, it must be the supremum of that system.

One consequence of the preceding remarks is that if X is an arbitrary subset of the universe of $\mathfrak{A}$, then the intersection of all those ideals that happen to include X is an ideal. (There is always at least one ideal that includes X, namely the improper ideal A.) That intersection—call it M—is the smallest ideal in $\mathfrak{A}$ that includes X; in other words, M is included in every ideal that includes X, by the very definition of the intersection that determines M. The ideal M is said to be *generated* by X, and X is called a *set of generators* for M. If Y is a subset of $\mathfrak{A}$ that includes X, then the ideal generated by Y obviously includes the ideal generated by X (because the ideal generated by Y includes Y and therefore also X, and the ideal generated by X is the smallest ideal that includes X). An ideal is said to be *finitely generated* if it is generated by some finite subset.

The definition just given of the ideal generated by a set X is top-down and non-constructive; it does not describe the elements in the ideal. (An advantage of the definition is that, with minimal changes,

it applies to every algebraic structure in which there is a suitable analogue of the notion of an ideal.) Fortunately, it is possible to give a more explicit description of the elements in the ideal.

Theorem 8.12. *In a relation algebra, an element r belongs to the ideal generated by a set X if and only if there is a finite subset Y of X such that $r \leq 1 ; (\sum Y) ; 1$.*

Proof. Fix a relation algebra $\mathfrak{A}$ and a subset X of $\mathfrak{A}$. Let M be the ideal generated in $\mathfrak{A}$ by X, and write

$$N = \{r : r \leq 1 ; (\textstyle\sum Y) ; 1 \text{ for some finite } Y \subseteq X\}. \tag{1}$$

It is to be shown that the sets M and N are equal. The proof makes use of the conditions in Definition 8.7 and Lemma 8.8.

Consider a finite subset Y of X. The sum $\sum Y$ belongs to M, by condition (ii), and therefore $1;(\sum Y);1$ belongs to M, by condition (iv). It follows that every element below $1 ; (\sum Y) ; 1$ belongs to M, by condition (v). Conclusion: N is a subset of M, by (1).

To establish the reverse inclusion, notice first that the set X is included in N. Indeed, an element r in X is always below $1 ; r ; 1$, by Lemma 4.5(iii) and its first dual, so r must be in N, by (1) (with Y taken to be the set $\{r\}$).

The next step is to check that N is an ideal. In view of Lemma 8.8, it suffices to verify conditions (i), (ii), (iv), and (v). The empty set is a finite subset of X, and its sum is 0. Since $0 = 1;0;1$, by Corollary 4.17 and its first dual, we conclude from (1) that 0 belongs to N. Thus, condition (i) is satisfied. Condition (v) obviously holds, by (1).

To verify condition (ii), consider elements r and s in N, say

$$r \leq 1 ; (\textstyle\sum Y) ; 1 \qquad \text{and} \qquad s \leq 1 ; (\textstyle\sum Z) ; 1,$$

where Y and Z are finite subsets of X. The union $Y \cup Z$ is a finite subset of X, and

$$r + s \leq [1 ; (\textstyle\sum Y) ; 1] + [1 ; (\textstyle\sum Z) ; 1] = 1 ; [\textstyle\sum (Y \cup Z)] ; 1,$$

by Boolean algebra and the distributive law for relative multiplication. Consequently, the sum $r + s$ is in N, by (1).

To verify condition (iv), consider an arbitrary element s in $\mathfrak{A}$ and an element r in N, say $r \leq 1 ; (\sum Y) ; 1$, where Y is a finite subset of X. The associative and monotony laws for relative multiplication imply that

$$r\,;s \leq [1\,;(\sum Y)\,;1]\,;s = [1\,;(\sum Y)]\,;(1\,;s) \leq 1\,;(\sum Y)\,;1.$$

Consequently, the product $r\,;s$ belongs to N, by (1). The argument that the product $s\,;r$ is in N is completely analogous.

It has been shown that N is an ideal and X is included in N. The set M is the smallest ideal that includes X, so M must be included in N. Thus, M and N are equal, as claimed. □

We turn now to the problem of describing all finitely generated ideals. The description of the ideal generated by the empty set is easy: it is just the trivial ideal $\{0\}$. Consider the next most complicated case, when M is an ideal generated by a single element s. Such an ideal is said to be *principal*. Theorem 8.12 implies that the ideal M consists of the elements that are below the ideal element $r = 1;s;1$ (see Section 5.5). Consequently, we have the following description of M.

Corollary 8.13. *An ideal M in a relation algebra is principal if and only if M has a largest element. That largest element r, if it exists, is an ideal element, and M is the set of elements that are below r.*

The principal ideal generated by an ideal element r is usually denoted by (r). Notice that both the trivial ideal and the improper ideal are principal; the former is generated by the ideal element 0, and the latter by the ideal element 1.

The preceding discussion clarifies why elements of the form $1\,;s\,;1$ are called ideal elements, and it also explains why only ideal elements are usually considered when speaking about generators of principal ideals.

Consider finally the general case of an arbitrary finitely generated ideal. Rather surprisingly, every such ideal must be principal.

Corollary 8.14. *Every finitely generated ideal in a relation algebra is principal.*

Proof. Let M be an ideal generated by a finite set X. If Y is any finite subset of X, then the sum $\sum Y$ is below the sum $\sum X$, and therefore the ideal element $1\,;(\sum Y)\,;1$ is below the ideal element

$$r = 1\,;(\sum X)\,;1,$$

by the monotony law for relative multiplication. Notice that r belongs to M, because the set X is assumed to be finite. Apply Theorem 8.12 to conclude that r is the largest element in M, and that M consists of all elements below r. Thus, $M = (r)$. □

In order to extend a given ideal M to a larger ideal, it is often helpful to proceed in a stepwise fashion, adjoining one element at a time and forming the ideal that is generated by this adjunction at each step. Theorem 8.12 implies that when adjoining a new element r_0, no generality is lost in assuming that r_0 is an ideal element. The next lemma describes the resulting *one-step extension*.

Lemma 8.15. *If M is an ideal, and r_0 an ideal element, in a relation algebra, then the ideal generated by $M \cup \{r_0\}$ is just the set*

$$N = \{r + s : r \leq r_0 \text{ and } s \in M\}.$$

Proof. Let L be the ideal generated by the set $M \cup \{r_0\}$. It is obvious from condition (ii) in the definition of an ideal, and condition (v) in Lemma 8.8, that the set N is included in L. To establish the reverse inclusion, consider an arbitrary element t in L. There must be a finite subset Y of $M \cup \{r_0\}$ such that $t \leq 1 ; (\sum Y) ; 1$, by Theorem 8.12. Without loss of generality, it may be assumed that r_0 is in Y. Each element u in Y that is different from r_0 belongs to M, and therefore so does the ideal element that is generated by u, by condition (iv) in the definition of an ideal. It follows that the sum

$$s_0 = \sum\{1 ; u ; 1 : u \in Y \sim \{r_0\}\}$$

belongs to M, by condition (ii). The distributive law for relative multiplication, the definition of s_0, and the fact that $1 ; r_0 ; 1 = r_0$ together imply that $t \leq r_0 + s_0$. Write

$$r = r_0 \cdot t \qquad \text{and} \qquad s = s_0 \cdot t,$$

and observe that r is below r_0, and s is in M, by condition (iii) in the definition of an ideal. Obviously,

$$t = (r_0 + s_0) \cdot t = r_0 \cdot t + s_0 \cdot t = r + s,$$

so t is in N. Thus, L is included in N. □

It is important to determine under what conditions a one-step extension of a proper ideal M continues to be a proper ideal. The next lemma answers this question.

Lemma 8.16. *Suppose M is an ideal, and r_0 an ideal element, in a relation algebra. The ideal generated by the set $M \cup \{r_0\}$ is proper if and only if $-r_0$ does not belong to M.*

Proof. The argument proceeds by contraposition. Assume first that the complement $-r_0$ belongs to M. The ideal N generated by $M \cup \{r_0\}$ then contains both r_0 and $-r_0$, so it contains the sum of these two elements, which is 1. Consequently, N is improper.

Now assume that N is improper. In this case, N contains the complement $-r_0$, so there must be an element $r \leq r_0$ and an element s in M such that $-r_0 = r+s$, by Lemma 8.15. Form the product of both sides of this equation with $-r_0$, and use Boolean algebra to obtain

$$\begin{aligned} -r_0 = -r_0 \cdot -r_0 = -r_0 \cdot (r+s) \\ = -r_0 \cdot r + -r_0 \cdot s = 0 + -r_0 \cdot s = -r_0 \cdot s. \end{aligned}$$

The equality of the first and last terms implies that $-r_0 \leq s$. Since s belongs to M, the complement $-r_0$ must belong to M as well, by condition (v) in Lemma 8.8. □

8.8 Lattice of ideals

The relation of one ideal being included in another is a partial order on the set of all ideals in a relation algebra $\mathfrak{A}$, and under this partial order the set of ideals in $\mathfrak{A}$ becomes a complete lattice. The infimum, or meet, of a system $(M_i : i \in I)$ of ideals is just the intersection $\bigcap_i M_i$ of the ideals in the system. The supremum, or join, of the system is, however, generally not the union $\bigcup_i M_i$ of the ideals in the system, since this union is rarely an ideal. Rather, the supremum is the ideal generated by the union $\bigcup_i M_i$; in other words, it is the intersection of the system of ideals that include every ideal M_i. We write $M \vee N$ and $M \wedge N$ for the join and meet of two ideals M and N, and $\bigvee_i M_i$ and $\bigwedge_i M_i$ for the join and meet of a system of ideals $(M_i : i \in I)$, in the lattice of ideals of some relation algebra.

It is worthwhile formulating a simple but quite useful alternative description of the join and meet of two ideals.

Lemma 8.17. *If M and N are ideals in a relation algebra, then*

$$M \vee N = \{r + s : r \in M \text{ and } s \in N\}$$

and

$$M \wedge N = \{r \cdot s : r \in M \text{ and } s \in N\}.$$

Proof. The proof makes use of the four conditions (i)–(iv) in the definition of an ideal, and condition (v) in Lemma 8.8. Let L be the complex sum of the ideals M and N,

$$L = \{r + s : r \in M \text{ and } s \in N\}.$$

It must be shown that $L = M \vee N$.

An element t in L has, by definition, the form $t = r + s$ for some elements r in M and s in N. The ideal $M \vee N$ includes both M and N, so it contains both r and s, and therefore it contains the sum t, by condition (ii). It follows that every element in L belongs to $M \vee N$, so L is certainly included in $M \vee N$.

To establish the reverse inclusion, consider an element t in the ideal $M \vee N$. Since $M \vee N$ is generated by the set $M \cup N$, there must exist some finite subsets X of M and Y of N such that t is below the product $1 ; [\sum(X \cup Y)] ; 1$, by Theorem 8.12. The elements

$$r = 1 ; (\textstyle\sum X) ; 1 \qquad \text{and} \qquad s = 1 ; (\textstyle\sum Y) ; 1$$

belong to M and N respectively, by conditions (ii) and (iv). It follows that the elements

$$p = r \cdot t \qquad \text{and} \qquad q = s \cdot t$$

are also in M and N respectively, by condition (iii). We have

$$t \leq 1 ; [\textstyle\sum(X \cup Y)] ; 1 = [1 ; (\sum X) ; 1] + [1 ; (\sum Y) ; 1] = r + s,$$

and therefore

$$t = (r + s) \cdot t = r \cdot t + s \cdot t = p + q.$$

Thus, t is the sum of an element from M and an element from N, so t must belong to L, by the definition of L. Because this is true for every element t in $M \vee N$, the join $M \vee N$ is included in L.

Now let L be the complex product of the ideals M and N,

$$L = \{r \cdot s : r \in M \text{ and } s \in N\}.$$

The goal is to show that $L = M \wedge N$.

An element t in $M \wedge N$ must belong to both M and N, since

$$M \wedge N = M \cap N.$$

The Boolean law $t = t \cdot t$ and the definition of L therefore imply that t is in L. Thus, every element in $M \wedge N$ belongs to L, so $M \wedge N$ is included in L.

To establish the reverse inclusion, consider an arbitrary element t in L. By definition, t has the form $t = r \cdot s$ for some elements r in M and s in N. In particular, t belongs to both ideals M and N, by condition (iii), so t belongs to the intersection of these two ideals, which is $M \wedge N$. Thus, each element in L is also in $M \wedge N$, so L is included in $M \wedge N$. □

The preceding lemma assumes a particularly perspicuous form when applied to principal ideals.

Corollary 8.18. *If r and s are ideal elements in a relation algebra, then*

$$(r) \vee (s) = (r + s) \qquad \textit{and} \qquad (r) \wedge (s) = (r \cdot s).$$

A generalization of the preceding corollary to arbitrary infinite systems of ideal elements is not valid, but the following weaker version does hold.

Lemma 8.19. *Suppose r is an ideal element, and $(r_i : i \in I)$ a system of ideal elements, in a relation algebra.*

(i) $(r) = \bigvee_i (r_i)$ *implies* $r = \sum_i r_i$.
(ii) $(r) = \bigwedge_i (r_i)$ *if and only if* $r = \prod_i r_i$.

Proof. The assumption in (i) implies that r belongs to the ideal generated by the system $(r_i : i \in I)$. Apply Theorem 8.12 to obtain a finite subset J of I such that

$$r \leq 1 \,;\, (\textstyle\sum_{i \in J} r_i) \,;\, 1.$$

Since

$$1 \,;\, (\textstyle\sum_{i \in J} r_i) \,;\, 1 = \textstyle\sum_{i \in J} (1 \,;\, r_i \,;\, 1) = \textstyle\sum_{i \in J} r_i,$$

by the distributive law for relative multiplication and the assumption that r_i is an ideal element for each i, it follows that

$$r \leq \textstyle\sum_{i \in J} r_i. \tag{1}$$

The assumption in (i) also implies that each ideal (r_i) is included in the ideal (r), and therefore each ideal element r_i is below r. Combine this with (1) to conclude that $r = \sum_{i \in I} r_i$.

Turn now to the proof of (ii). Write

$$M = \bigwedge_i (r_i) = \bigcap_i (r_i). \tag{2}$$

Assume first that $r = \prod_i r_i$. In this case r is below each element r_i, so r belongs to each ideal (r_i), and therefore (r) is included in the meet M of these ideals. On the other hand, if s is an element in M, then s is in the ideal (r_i) for each index i, by (2). Therefore, s is below each ideal element r_i, so s is below the infimum r of these ideal elements. It follows that s belongs to (r). This establishes the implication from left to right in (ii).

To establish the reverse implication, assume that $(r) = M$. In this case, r belongs to each ideal (r_i), by (2), so r is below each element r_i. If s is any element that is below each r_i, then s belongs to each of the ideals (r_i), and therefore s belongs to M, by (2). It follows that s is in (r) and consequently below r. Thus, r is the greatest lower bound of the set of ideal elements r_i. □

The lattice of ideals in a relation algebra is not only complete, it is also distributive in the sense that joins distribute over meets, and meets over joins. The proof is a direct application of Lemma 8.17. Let L, M, and N be three ideals in a relation algebra. Lemma 8.17 implies that

$$L \vee (M \wedge N) = \{r + (s \cdot u) : r \in L,\ s \in M, u \in N\}$$

and

$$(L \vee M) \wedge (L \vee N) = \{(r + t) \cdot (s + u) : r, s \in L,\ t \in M, u \in N\}.$$

Since

$$r + (s \cdot u) = (r + s) \cdot (r + u),$$

by the distributive law for addition over multiplication, every element in the first ideal is also in the second.

The proof of the reverse inclusion is a bit more involved. Let v be an arbitrary element in the second ideal, say

$$v = (r + t) \cdot (s + u),$$

where r and s are in L, and t and u are in M and N respectively. Apply the Boolean distributive and monotony laws to obtain

$$\begin{aligned} v = (r+t)\cdot(s+u) &= (r\cdot s)+(r\cdot u)+(t\cdot s)+(t\cdot u) \\ &\le r+r+s+(t\cdot u) = (r+s)+(t\cdot u). \end{aligned}$$

The sum $r+s$ is in L, by condition (ii) in the definition of an ideal, and the elements t and u are in M and N respectively, so the product $t\cdot u$ belongs to the ideal $M \wedge N$, by Lemma 8.17. The sum $(r+s)+(t\cdot u)$ therefore belongs to the first ideal defined above. Since v is below this sum, it too belongs to the first ideal, by condition (v) in Lemma 8.8. Conclusion:

$$L \vee (M \wedge N) = (L \vee M) \wedge (L \vee N).$$

The dual distributive law

$$L \wedge (M \vee N) = (L \wedge M) \vee (L \wedge N)$$

can be established in a similar fashion, or it can be derived directly from the preceding law.

Let us return for a moment to the question of the join of a system of ideals. As was mentioned earlier, the union of a system of ideals usually fails to be an ideal. There is, however, an exception. A non-empty system $(M_i : i \in I)$ of ideals in a relation algebra is said to be *directed* if any two ideals M_i and M_j in the system are included in some third ideal M_k in the system.

Lemma 8.20. *The union of a non-empty, directed system of ideals in a relation algebra* $\mathfrak{A}$ *is again an ideal in* $\mathfrak{A}$, *and this ideal is proper if and only if each ideal in the system is proper.*

Proof. The proof is similar to that of Lemma 6.7. Consider a non-empty, directed system $(M_i : i \in I)$ of ideals in $\mathfrak{A}$, and let M be the union of the ideals in this system. It is to be shown that M satisfies conditions (i)–(iv) of Definition 8.7. Certainly, 0 belongs to M, because 0 belongs to each ideal in the given system, and the system is assumed to be non-empty. Thus, condition (i) is satisfied.

To verify condition (ii), consider elements r and s in M. There must be indices i and j in I such that r is in M_i and s in M_j, by the definition of M. The two ideals M_i and M_j are included in some third ideal M_k in the system, because the system is assumed to be directed. The elements r and s therefore both belong to M_k, and consequently so does their sum $r+s$, since M_k is assumed to be an ideal. It follows that this sum belongs to M, as desired.

The verification of conditions (iii) and (iv) is easier. Suppose r is an element in M, and s an element in $\mathfrak{A}$. There must be an index i in I such that r is in M_i. The elements $r \cdot s$, $r\,;s$, and $s\,;r$ all belong to M_i, by the assumption that M_i is an ideal. Consequently, these elements all belong to M, by the definition of M.

The ideal M is proper if and only if each ideal M_i in the system is proper, because M is the union of the ideals M_i, and the union does not contain the element 1 if and only if each M_i does not contain 1. □

The lemma applies, in particular, to non-empty *chains* of ideals, that is to say, to non-empty systems of ideals that are linearly ordered by the relation of inclusion.

Corollary 8.21. *The union of a non-empty chain of ideals in a relation algebra $\mathfrak{A}$ is again an ideal in $\mathfrak{A}$, and this ideal is proper if and only if each ideal in the chain is proper.*

Consider now an arbitrary ideal M. Each element t in M is below the generated ideal element $r = 1\,;t\,;1$, by Lemma 4.5(iii) and its first dual. Also, r belongs to M, by condition (iv) in the definition of an ideal, and therefore the principal ideal generated by r is included in M. It follows that M is the union of the system of principal ideals generated by the ideal elements in M. This system is directed. Indeed, for any two ideal elements r and s in M, the sum $r + s$ is an ideal element that is also in M, by Lemma 5.39(ii) and Definition 8.7(ii), and the principal ideals (r) and (s) are both included in the principal ideal $(r + s)$. Conclusion: every ideal in a relation algebra is the union of a directed system of principal ideals.

An ideal M is defined to be a *compact element* in the lattice of ideals in a relation algebra provided that whenever M is included in the join of some system of ideals, it is already included in the join of finitely many of the ideals in the system. A principal ideal (r) is always a compact element. For the proof, suppose that (r) is included in the join of a system $(M_i : i \in I)$ of ideals. The element r belongs to this join, so there must be a finite subset Y of the union $\bigcup_{i\in I} M_i$ such that r is below the ideal element $s = 1\,;(\sum Y)\,;1$, by Theorem 8.12. Since Y is finite, there must be a finite subset J of the index set I such that Y is included in the union $\bigcup_{i\in J} M_i$. Apply Theorem 8.12 again to conclude that r belongs to the join of the finite system $(M_i : i \in J)$, and therefore (r) is included in this join.

Conversely, every compact element in the lattice of ideals in a relation algebra is necessarily principal. Indeed, an ideal M is equal to

the join of a directed system of principal ideals, by the observations of the preceding paragraph. If M is compact, then M must be included in, and therefore equal to, the join of finitely many of these principal ideals. The join of finitely many principal ideals is again a principal ideal, by Corollary 8.18 and Lemma 5.39(ii), so M is a principal ideal.

As we have already seen, every ideal is the join of a direct family of principal ideals, so it follows from the observations of the preceding paragraphs that every ideal is the join of compact elements. Thus, the lattice of ideals in a relation algebra is compactly generated. We summarize the preceding observations in the following theorem.

Theorem 8.22. *The ideals in a relation algebra form a complete, compactly generated, distributive lattice that is closed under directed unions. The join and meet of two ideals are their complex sum and product respectively. The compact elements are the principal ideals.*

In view of the close connection between congruences and ideals, it should come as no surprised that the lattice of congruences is isomorphic to the lattice of ideals.

Theorem 8.23. *The function that maps each congruence on a relation algebra $\mathfrak{A}$ to its kernel is an isomorphism from the lattice of congruences on $\mathfrak{A}$ to the lattice of ideals in $\mathfrak{A}$.*

Proof. Every congruence on $\mathfrak{A}$ uniquely determines its kernel, which is an ideal, by the observations at the beginning of Section 8.6. Also, every ideal in $\mathfrak{A}$ is the kernel of exactly one congruence, by Theorem 8.9. Consequently, the function mapping each congruence on $\mathfrak{A}$ to its kernel is a bijection from the lattice of congruences on $\mathfrak{A}$ to the lattice of ideals in $\mathfrak{A}$.

In order to establish the preservation properties required of a lattice isomorphism, it suffices to show that the bijection under consideration preserves the relation of inclusion in the following sense: if Θ and Φ are congruences on $\mathfrak{A}$, and if M and N are their respective kernels, then

$$\Theta \subseteq \Phi \qquad \text{if and only if} \qquad M \subseteq N.$$

To say that Θ is included in Φ means that whenever elements r and s are congruent modulo Θ, they are also congruent modulo Φ. In particular, whenever r and 0 are congruent modulo Θ, they are also congruent modulo Φ. This is just another way of saying that the kernel M is included in the kernel N. On the other hand if M is included in N, then

whenever a symmetric difference $r \ominus s$ belongs to M, this symmetric difference must also belong to N. This is just another way of saying that whenever elements r and s are congruent modulo Θ, they are also congruent modulo Φ, by Theorem 8.9; and this in turn means that Θ is included in Φ. □

One consequence of Theorems 8.22 and 8.23 is that the lattice of congruences on a relation algebra is actually distributive, and not just modular; see the remark after Theorem 8.3.

8.9 Ideal elements and ideals

Theorem 8.12, Corollary 8.18, and the remarks leading up to Theorem 8.22 hint at a very close connection between the ideals and the ideal elements in a relation algebra. We now pursue this connection further. The following observation was already made informally before Lemma 5.40.

Lemma 8.24. *The set of ideal elements in a relation algebra $\mathfrak{A}$ is a strongly regular Boolean subalgebra of the Boolean part of $\mathfrak{A}$.*

Corollary 8.25. *If a relation algebra $\mathfrak{A}$ is complete, then the Boolean algebra of ideal elements in $\mathfrak{A}$ is a complete Boolean subalgebra of the Boolean part of $\mathfrak{A}$.*

Rather surprisingly, it turns out that the lattice of ideals in a relation algebra $\mathfrak{A}$ is isomorphic to the lattice of Boolean ideals in the Boolean algebra of ideal elements in $\mathfrak{A}$. To see this, write B for the set of ideal elements in $\mathfrak{A}$. A relation algebraic ideal M in $\mathfrak{A}$ is also a Boolean ideal in the Boolean part of $\mathfrak{A}$, by conditions (i)–(iii) in Definition 8.7. The intersection

$$B_M = B \cap M$$

must therefore be a Boolean ideal in B, because the intersection of a Boolean ideal with a Boolean subalgebra is always a Boolean ideal in the subalgebra.

Conversely, if K is a Boolean ideal in B, then the set

$$A_K = \{r \in A : 1 ; r ; 1 \in K\} = \{r \in A : r \leq s \text{ for some } s \in K\}$$

is easily seen to be a relation algebraic ideal in $\mathfrak{A}$. For example, to check one half of condition (iv) in Definition 8.7, consider an element r

in A_K and an arbitrary element t in $\mathfrak{A}$. The definition of A_K implies that $r \leq s$ for some element s in K. Therefore,

$$r\,;t \leq s\,;1 = s,$$

by the monotony law for relative multiplication and the fact that the ideal element s is a right ideal element (see Lemma 5.38(vi)). Consequently, $r\,;t$ belongs to the set A_K, by the definition of this set.

Start with an ideal M in $\mathfrak{A}$, form the Boolean ideal B_M, and then form the relation algebraic ideal A_{B_M}; the result is just the original ideal M. In other words,

$$A_{B_M} = M.$$

For the proof, consider an arbitrary element r in $\mathfrak{A}$, let $s = 1\,;r\,;1$, and observe that $r \leq s$, by Lemma 4.5(iii) and its first dual. If r is in M, then s is in M, by condition (iv) in Definition 8.7; since s is also in B, by the definition of B, it follows that s belongs to the intersection of B and M, which is just B_M. Consequently, r must belong to A_{B_M}, by the definition of the set A_K (with B_M in place of K). Conversely, if r is in A_{B_M}, then s belongs to the set B_M, by the definition of A_K, and therefore s belongs to the ideal M (and to B), by the definition of B_M. Consequently, r belongs to M, by condition (v) in Lemma 8.8.

An entirely analogous argument shows that if we start with a Boolean ideal K in B, form the relation algebraic ideal A_K, and then form the Boolean ideal B_{A_K}, we arrive at the original Boolean ideal K. In other words,

$$B_{A_K} = K.$$

Conclusion: the function mapping each ideal M in $\mathfrak{A}$ to the Boolean ideal B_M in B, and the function mapping each Boolean ideal K in B to the ideal A_K in $\mathfrak{A}$ are inverses of one another, and are therefore bijections.

If M and N are ideals in $\mathfrak{A}$, and if M is included in N, then obviously

$$B \cap M \subseteq B \cap N,$$

so that B_M is included in B_N. Conversely, if K and L are ideals in B, and if K is included in L, then A_K is included in A_L, since

$$\{r \in A : r \leq s \text{ for some } s \in K\} \subseteq \{r \in A : r \leq s \text{ for some } s \in L\}.$$

In particular, if B_M is included in B_N, then A_{B_M} is included in A_{B_N}, and therefore M is included in N. Conclusion:

$$B_M \subseteq B_N \qquad \text{if and only if} \qquad M \subseteq N.$$

These observations lead to the following important theorem, called the *Lattice of Ideals Theorem.*

Theorem 8.26. *Let* $\mathfrak{A}$ *be a relation algebra and* B *the Boolean algebra of ideal elements in* $\mathfrak{A}$. *The function mapping each ideal* M *in* $\mathfrak{A}$ *to the Boolean ideal* $B \cap M$ *is an isomorphism from the lattice of ideals in* $\mathfrak{A}$ *to the lattice of Boolean ideals in* B. *The inverse of this function maps each Boolean ideal* K *in* B *to the ideal* $\{r \in A : \ 1 ; r ; 1 \in K\}$ *in* $\mathfrak{A}$.

The lattice of ideals in a Boolean algebra is known to be complete, compactly generated, and distributive (see, for example, [38]), so the corresponding result for the lattice of ideals in a relation algebra—that is to say, part of the first assertion in Theorem 8.22—follows at once from the preceding theorem. Any lattice isomorphism must map compact elements to compact elements, since the property of being compact can be expressed lattice-theoretically. It follows that the isomorphism in the preceding theorem maps the finitely generated relation algebraic ideals to finitely generated Boolean ideals. In other words, it maps principal ideals to principal Boolean ideals. Here is another way of seeing the same thing. A relation algebraic ideal M is principal if and only if it has a largest element, which is necessarily an ideal element. The corresponding Boolean ideal, say K, consists of the ideal elements in M, so if M has a largest element, then K has the same largest element, and vice versa.

Corollary 8.27. *An ideal in a relation algebra is principal just in case the corresponding Boolean ideal* (*in the Boolean algebra of ideal elements*) *is principal. If these ideals are principal*, *then they are generated by the same ideal element.*

We close this section with one more observation about the Boolean algebra of ideal elements, namely if a relation algebra is atomic, then so is its Boolean algebra of ideal elements. The corresponding remark about atomless algebras is false.

Lemma 8.28. *If* r *is an atom in a relation algebra* $\mathfrak{A}$, *then* $1 ; r ; 1$ *is an atom in the corresponding Boolean algebra of ideal elements. Consequently*, *if* $\mathfrak{A}$ *is atomic*, *then so is the Boolean algebra of ideal elements in* $\mathfrak{A}$.

Proof. Two applications of the De Morgan-Tarski equivalences (see Lemma 4.8), combined with Lemma 4.1(vi), imply that, for any elements r and s in $\mathfrak{A}$,

$$(1\,;r\,;1)\cdot s \neq 0 \qquad \text{if and only if} \qquad (1\,;s\,;1)\cdot r \neq 0. \tag{1}$$

To prove the first assertion of the theorem, assume that r is an atom in $\mathfrak{A}$. Certainly, $1\,;r\,;1$ is not zero, since $r \leq 1\,;r\,;1$, by Lemma 4.5(iii) and its first dual. If s is an ideal element whose product with $1\,;r\,;1$ is non-zero, then the product of r with $1\,;s\,;1$ is non-zero, by (1). Since $1\,;s\,;1 = s$, by the definition of an ideal element (see Section 5.5), it follows that $r\cdot s$ is non-zero, and therefore $r \leq s$, because r is assumed to be atom. Form the relative product of both sides of this inequality with 1 on the left and the right, and use the monotony law for relative multiplication and the definition of an ideal element to arrive at

$$1\,;r\,;1 \leq 1\,;s\,;1 = s. \tag{2}$$

Conclusion: for any ideal element s, the ideal element $1\,;r\,;1$ is either disjoint from s or below s. This is precisely what it means for $1\,;r\,;1$ to be an atom in the Boolean algebra of ideal elements.

Now assume that $\mathfrak{A}$ is atomic. For each non-zero ideal element s, there is an atom r in $\mathfrak{A}$ that is below s, by the assumed atomicity of $\mathfrak{A}$. The generated ideal element $1\,;r\,;1$ is an atom below s in the Boolean algebra of ideal elements, by (2) and the observations of the previous paragraph. Consequently, the Boolean algebra of ideal elements in $\mathfrak{A}$ is atomic. □

8.10 Maximal ideals

An ideal in a relation algebra is said to be *maximal* if it is a proper ideal that is not properly included in any other proper ideal. Equivalently, to say that an ideal M is maximal in a relation algebra $\mathfrak{A}$ means that $M \neq A$, and for any ideal N in $\mathfrak{A}$,

$$M \subseteq N \subseteq A \qquad \text{implies} \qquad N = M \text{ or } N = A.$$

Thus, maximal ideals in $\mathfrak{A}$ are just maximal elements in the lattice of ideals in $\mathfrak{A}$. More generally, an ideal M is said to be *maximal in an ideal* L if M is properly included in L, and M is not properly included in

any other ideal that is properly included in L. Using this terminology, maximal ideals may be described as ideals that are maximal in the improper ideal A.

Maximal ideals are characterized by some curious algebraic properties.

Lemma 8.29. *The following conditions on an ideal M in a relation algebra $\mathfrak{A}$ are equivalent.*

(i) *The ideal M is maximal.*
(ii) *For every ideal element r in $\mathfrak{A}$, exactly one of r and $-r$ belongs to M.*
(iii) *For every element r in $\mathfrak{A}$, exactly one of r and $-(1\,;r\,;1)$ belongs to M.*
(iv) *The ideal M is proper, and for every pair of elements r and s in $\mathfrak{A}$, if $r\,;1\,;s$ is in M, then either r or s is in M.*

Proof. The proof proceeds by showing that condition (ii) is equivalent to each of the other three conditions. The following preliminary remarks (consequences of conditions (ii) and (iv) in Definition 8.7 and condition (v) in Lemma 8.8) are used several times. First, the ideal M is improper if and only if, for some element r in $\mathfrak{A}$, both r and $-r$ belong to M. Second, for all elements r in $\mathfrak{A}$,

$$r \in M \qquad \text{if and only if} \qquad 1\,;r\,;1 \in M. \tag{1}$$

To establish the equivalence of (i) and (ii), assume first that condition (i) holds, and consider an arbitrary ideal element r in $\mathfrak{A}$. Suppose that the complement $-r$ is not in M. In this case, the set $M \cup \{r\}$ can be extended to a proper ideal N, by Lemma 8.16. The assumption that M is maximal implies that $N = M$, so r must belong M. Clearly, r and $-r$ cannot both be in M, for then M would be an improper ideal, by the preliminary remarks above. Thus, condition (ii) holds.

Assume now that condition (ii) holds. The ideal M is certainly proper, because the element 0 is in M, by Definition 8.7(i), and therefore the complement of this element, namely 1, cannot be in M, by condition (ii). Consider now an arbitrary ideal N in $\mathfrak{A}$ that properly includes M. There must be an element r in N that does not belong to M, by the assumption that N is a proper extension of M; and it may be supposed, by (1), that r is an ideal element. Since r is not in M, the complement $-r$ must be in M, by condition (ii), and therefore $-r$

is also in N, by the assumption that N includes M. The ideal N therefore contains both r and $-r$, so N is an improper ideal. Conclusion: M is a proper ideal, and the only proper extension of M is the improper ideal. Thus, condition (i) holds.

The equivalence of conditions (ii) and (iii) is an immediate consequence of (1) and the definition of an ideal element.

To establish the equivalence of (ii) and (iv), assume first that condition (iv) holds, and consider an arbitrary ideal element r in $\mathfrak{A}$. We have

$$r\,;1\,;-r = r\,;-r = r \cdot -r = 0,$$

by Lemmas 5.38(vi), 5.39(ii), 5.41(ii), and Boolean algebra. Consequently, the element $r\,;1\,;-r$ belongs to M, by Definition 8.7(i). Apply condition (iv) to obtain that at least one of the elements r and $-r$ is in M. They cannot both be in M, because M is assumed to be a proper ideal. Thus, condition (ii) holds.

To establish the reverse implication, assume that condition (ii) holds. It has already been observed that in this case the ideal M must be proper. Consider an element of the form $r\,;1\,;s$ that belongs to M. The generated ideal element $1\,;r\,;1\,;s\,;1$ is then in M, by (1). Since

$$\begin{aligned} 1\,;r\,;1\,;s\,;1 &= 1\,;r\,;1\,;1\,;s\,;1 \\ &= (1\,;r\,;1)\,;(1\,;s\,;1) = (1\,;r\,;1)\cdot(1\,;s\,;1), \end{aligned}$$

by Lemma 4.5(iv), the associative law for relative multiplication, and Lemma 5.41(ii), the product

$$(1\,;r\,;1)\cdot(1\,;s\,;1) \tag{2}$$

must in M. Assume now that r is not in M. In this case, the ideal element $1\,;r\,;1$ cannot be in M, by (1), so its complement $-(1\,;r\,;1)$ must be in M, by condition (ii). Add this complement to (2), and use Definition 8.7(ii), to conclude that the sum

$$-(1\,;r\,;1) + (1\,;r\,;1)\cdot(1\,;s\,;1)$$

is in M. The ideal element $1\,;s\,;1$ is below this sum, so it, too, must be in M, and therefore s must be in M, by (1). Thus, condition (iv) holds. □

The main result concerning maximal ideals is that they exist in profusion: every proper ideal is included in a maximal ideal. The next theorem contains a stronger version of this statement.

Theorem 8.30. *If L is a principal ideal in a relation algebra, and M an ideal that is properly included in L, then there is an ideal that is maximal in L and includes M.*

Proof. Assume $L = (r)$, where r is an ideal element in a relation algebra $\mathfrak{A}$, and let M be an ideal that is properly included in L. Consider the set W of all ideals in $\mathfrak{A}$ that include M and are properly included in L. It is not difficult to check that the union of any non-empty chain of ideals in W is again an ideal in W. For the proof, suppose that N is the union of some non-empty chain of ideals in W. Certainly, N is an ideal, by Corollary 8.21. Also, N obviously includes M, because the chain is assumed to be non-empty and every ideal in the chain includes M, by the definition of W. Finally, N is properly included in L, because N cannot contain the element r, since no ideal in the chain contains r, by assumption. Therefore N belongs to W, by the definition of W.

Apply Zorn's Lemma to conclude that W has a maximal element. The definition of W implies that this maximal element is an ideal that includes M and is maximal in L. □

An alternative proof of the preceding theorem uses the Lattice of Ideals Theorem 8.26 from the preceding section. Here are the details. Let L_0 and M_0 be the images of the relation algebraic ideals L and M under the lattice isomorphism given in that theorem. Because the isomorphism maps principal ideals to principal Boolean ideals, and preserves inclusion, L_0 must be a principal Boolean ideal in the Boolean algebra of ideal elements, and M_0 must be a Boolean ideal that is properly included in L_0. Apply the well-known Boolean analogue of Theorem 8.30 to obtain a Boolean ideal N_0 that includes M_0 and is maximal in L_0. If N is the unique relation algebraic ideal in $\mathfrak{A}$ that is mapped to N_0 by the lattice isomorphism, then N includes M and is maximal in L, by the lattice preservation properties of the isomorphism.

The following important consequence of Theorem 8.30 is called the *Maximal Ideal Theorem*.

Theorem 8.31. *For every proper ideal M in a relation algebra, and every element r that does not belong to M, there is a maximal ideal that includes M and does not contain r.*

Proof. The ideal M does not contain the element r, by assumption, so M cannot contain the ideal element $1 ; r ; 1$, (see (1) in the proof of

Lemma 8.29). The ideal generated by the set

$$M \cup \{-(1\,;r\,;1)\} \tag{1}$$

is therefore proper, by Lemma 8.16 (with $-(1\,;r\,;1)$ in place of r_0). Apply Theorem 8.30, with the improper ideal (which is generated by the unit and is therefore principal) in place of L and with the ideal generated by (1) in place of M, to obtain an ideal N that includes (1) and is maximal in L. Since the ideal L is improper, the ideal N must be maximal; and since N contains $-(1\,;r\,;1)$, it cannot contain r, by Lemma 8.29(iii). □

We now make a few observations about the connections between principal ideals and maximal ideals. A bit of terminology will be helpful. Call an atom of the Boolean algebra of ideal elements in a relation algebra $\mathfrak{A}$ an *ideal element atom* in $\mathfrak{A}$. Warning: an ideal element atom in $\mathfrak{A}$ need not be an atom in $\mathfrak{A}$.

Lemma 8.32. *A principal ideal in a relation algebra is maximal if and only if it has the form* $(-s)$ *for some ideal element atom* s.

Proof. The lattice isomorphism in the Lattice of Ideals Theorem 8.26 maps maximal ideals to maximal ideals, and principal ideals to principal ideals. Consequently, the lemma follows directly from the fact that a principal Boolean ideal is maximal if and only if its generator is the complement of an atom. In more detail, a principal ideal (r) in the Boolean algebra of ideal elements is maximal just in case, for all ideal elements s, precisely one of s and $-s$ is in (r). In other words, exactly one of s and $-s$ is below r. This means that $-r$ is below exactly one of $-s$ and s, which is just the condition for r to be an atom in the Boolean algebra of ideal elements. □

The preceding lemma leads naturally to the problem of characterizing when a maximal ideal is non-principal.

Lemma 8.33. *A maximal ideal in a relation algebra contains all but at most one ideal element atom. It contains all ideal element atoms if and only if it is non-principal.*

Proof. A maximal ideal M in a relation algebra does not contain an ideal element atom s just in case M contains $-s$ and therefore coincides with $(-s)$, by Lemma 8.29 and the fact that $(-s)$ is a maximal

ideal (see Lemma 8.32). For distinct ideal element atoms s and t, the maximal ideals $(-s)$ and $(-t)$ must be distinct, since $-s$ and $-t$ are the largest elements in the ideals that they generate. Consequently, if M does not contain s, and therefore coincides with $(-s)$, then M cannot contain the complement of any other ideal element atom, and therefore M must contain every ideal element atom different from s, by Lemma 8.29. These observations imply that a maximal ideal M is non-principal if and only if it does not contain the complement of any ideal element atom, or, equivalently, if and only if it contains all ideal element atoms. □

We are now in a position to characterize the relation algebras that have maximal, non-principal ideals.

Theorem 8.34. *The following conditions on a relation algebra* $\mathfrak{A}$ *are equivalent.*

(i) *There are only finitely many ideal elements in* $\mathfrak{A}$.
(ii) *There are only finitely many ideals in* $\mathfrak{A}$.
(iii) *Every ideal in* $\mathfrak{A}$ *is principal.*
(iv) *Every maximal ideal in* $\mathfrak{A}$ *is principal.*

Proof. The proof proceeds by showing that condition (i) implies each of the other three conditions, and the negation of (i) implies the negation of each of the other three conditions. Suppose first that (i) holds. This condition says that the Boolean algebra B of ideal elements in $\mathfrak{A}$ is finite. A finite Boolean algebra can have only finitely many Boolean ideals, and each of these ideals must be finite. It follows that the sum of the elements in each of these Boolean ideal is again an element in the ideal, so every Boolean ideal in B is principal. Apply the Lattice of Ideals Theorem 8.26 and Corollary 8.27 to conclude that $\mathfrak{A}$ has only finitely many ideals, and each of these ideals is principal.

Assume now that the negation of condition (i) holds. This means that the Boolean algebra B is infinite. Clearly, B has as many principal Boolean ideals as it has elements, so B has infinitely many principal Boolean ideals, and therefore $\mathfrak{A}$ has infinitely many principal ideals, by the Lattice of Ideals Theorem and Corollary 8.27.

We proceed to construct a maximal ideal in $\mathfrak{A}$ that is not principal. Let X be the set of atoms in B, and let M be the ideal generated in $\mathfrak{A}$ by X. An element r in $\mathfrak{A}$ belongs to M if and only if there is a finite subset Y of X such that

$$r \leq 1 ; (\sum Y) ; 1 = \sum\{1 ; s ; 1 : s \in Y\} = \sum Y,$$

by Theorem 8.12, the distributivity of relative multiplication, and the definition of an ideal element, together with the assumption that X, and therefore also Y, consists of ideal elements in $\mathfrak{A}$. The assumption that there are infinitely many ideal elements in $\mathfrak{A}$ implies that 1 cannot be the sum of a finite subset of X. Indeed, an arbitrary Boolean algebra is finite if and only if its unit is the sum of finitely many atoms, and we have assumed that B is infinite. Consequently, 1 cannot be in M, so M is a proper ideal.

Use the Maximal Ideal Theorem to extend M to a maximal ideal N in $\mathfrak{A}$. Every ideal element atom, that is to say, every element in X, belongs to M and therefore also to N. Apply Lemma 8.33 to conclude that the maximal ideal N is not principal. □

We shall see in Corollary 11.42 that another condition involving direct products is equivalent to each of the conditions in the preceding theorem, namely that the relation algebra $\mathfrak{A}$ is isomorphic to the direct product of finitely many simple algebras.

Corollary 8.35. *A relation algebra $\mathfrak{A}$ has maximal ideals that are non-principal if and only if $\mathfrak{A}$ has infinitely many ideal elements.*

8.11 Homomorphism and isomorphism theorems

The connection between congruences and homomorphisms (discussed in Section 8.5) implies a similar connection between ideals and homomorphisms. Indeed, the translation from the (informal) language of congruences to the language of ideals that was discussed at the end of Section 8.6 allows us to translate every result about quotients of relation algebras by congruences into a corresponding result about quotients of relation algebras by ideals. As an example, here is the translation of Lemma 8.4.

Lemma 8.36. *For every ideal M on a relation algebra $\mathfrak{A}$, the function mapping r to r/M for each r in $\mathfrak{A}$ is an epimorphism from $\mathfrak{A}$ to $\mathfrak{A}/M$.*

The mapping in the lemma is called the *canonical homomorphism*, or the *quotient homomorphism*, from $\mathfrak{A}$ to $\mathfrak{A}/M$. It is exactly the same mapping that was discussed in Lemma 8.4, so there is no inherent conflict in our use of this terminology in the present situation.

Corresponding to the notion of the congruence induced by a homomorphism, there is also a notion of the ideal induced by a homomorphism. In more detail, the *kernel* of a homomorphism φ on a relation algebra $\mathfrak{A}$ is the set of those elements in $\mathfrak{A}$ that are mapped to zero by φ. This kernel is easily seen to be an ideal. The proof involves a straightforward verification of the conditions in Definition 8.7. For example, if r is in the kernel of φ and if s is any element in $\mathfrak{A}$, then

$$\varphi(r\,;s) = \varphi(r)\,;\varphi(s) = 0\,;\varphi(s) = 0,$$

by the homomorphism properties of φ, the assumption that r is in the kernel, and the first dual of Corollary 4.17; consequently, $r\,;s$ is in the kernel. The other conditions in Definition 8.7 are verified in a similar fashion. Alternatively, one can observe that if Θ is the congruence induced by the homomorphism φ, then the kernel of φ coincides with the congruence class of 0 modulo Θ, so the kernel must be an ideal, by the remarks at the beginning of Section 8.6.

Here is a general and useful remark about homomorphisms and their kernels.

Lemma 8.37. *A homomorphism is a monomorphism if and only if its kernel is the trivial ideal* $\{0\}$.

Proof. Consider a homomorphism φ on a relation algebra. If φ is one-to-one, and if $\varphi(r) = 0$, then $\varphi(r) = \varphi(0)$ and therefore $r = 0$. Consequently, the kernel of φ is $\{0\}$.

On the other hand, if the kernel of φ is $\{0\}$, and if $\varphi(r) = \varphi(s)$, then

$$\varphi(r \ominus s) = \varphi(r) \ominus \varphi(s) = \varphi(r) \ominus \varphi(r) = 0,$$

so that $r \ominus s = 0$ and therefore $r = s$, by the assumption about the kernel. Consequently, φ is one-to-one. □

If the domain of a homomorphism φ is an atomic relation algebra, then the preceding lemma can be strengthened somewhat. In this case, a homomorphism is a monomorphism if and only if no atom belongs to the kernel. The necessity of the condition that the kernel not contain an atom is a consequence of the lemma. To establish the sufficiency of the condition, argue by contraposition. If the kernel contains a non-zero element r, then it must contain every atom s below r, because

$$\varphi(s) \leq \varphi(r) = 0.$$

Consequently, if the kernel does not contain an atom, then it cannot contain a non-zero element, by the assumption that the domain algebra is atomic, so the homomorphism φ must be one-to-one.

We have seen that the kernel of every homomorphism is an ideal. It is natural and important to raise the converse question: is every ideal the kernel of some homomorphism? The answer is easily seen to be yes: if M is an ideal in a relation algebra $\mathfrak{A}$, then the quotient mapping of $\mathfrak{A}$ onto $\mathfrak{A}/M$ is an epimorphism, by Lemma 8.36. The kernel of the quotient mapping is clearly M, since

$$\begin{aligned} r/M = 0/M \qquad &\text{if and only if} \qquad r \ominus 0 \in M, \\ &\text{if and only if} \qquad r \in M, \end{aligned}$$

because $r \ominus 0 = r$. This proves the following analogue of Theorem 8.5, known as the *Homomorphism Theorem* (for ideals).

Theorem 8.38. *Every ideal M in a relation algebra $\mathfrak{A}$ is the kernel of some epimorphism, namely the quotient homomorphism from $\mathfrak{A}$ to $\mathfrak{A}/M$.*

We saw in Theorem 8.6 that, up to isomorphism, the homomorphic images of a relation algebra $\mathfrak{A}$ are just the quotients of $\mathfrak{A}$ modulo the congruences on $\mathfrak{A}$. The next theorem, known as the *First Isomorphism Theorem* (for ideals) gives the version of this result that applies to ideals.

Theorem 8.39. *Every homomorphic image of a relation algebra $\mathfrak{A}$ is isomorphic to a quotient of $\mathfrak{A}$ modulo some ideal. In fact, if φ is an epimorphism from $\mathfrak{A}$ to $\mathfrak{B}$, and if M is the kernel of φ, then $\mathfrak{A}/M$ is isomorphic to $\mathfrak{B}$ via the function that maps r/M to $\varphi(r)$ for every element r in $\mathfrak{A}$.*

Proof. The theorem is exactly Theorem 8.6, formulated in the language of ideals instead of the language of congruences, so it follows at once from that theorem.

Alternatively, a direct proof of the theorem, avoiding any discussion of congruences, can be given by translating the proof of Theorem 8.6 into the language of ideals. For example, consider an epimorphism φ from $\mathfrak{A}$ to $\mathfrak{B}$, and let M be the kernel of φ. For elements r and s in $\mathfrak{A}$, we have

$$\begin{aligned}
\varphi(r) = \varphi(s) \qquad &\text{if and only if} \qquad \varphi(r) \ominus \varphi(s) = 0, \\
&\text{if and only if} \qquad \varphi(r \ominus s) = 0, \\
&\text{if and only if} \qquad r \ominus s \in M, \\
&\text{if and only if} \qquad r/M = s/M,
\end{aligned}$$

by the properties of symmetric difference (every element is its own inverse with respect to this operation), the homomorphism properties of φ, and the definition of the kernel M. If ψ is the function from $\mathfrak{A}/M$ to $\mathfrak{B}$ that is defined by

$$\psi(r/M) = \varphi(r)$$

for each element r in $\mathfrak{A}$ (see Figure 8.1), then the preceding computation implies that ψ is a well-defined bijection. The proof that ψ preserves the operations of $\mathfrak{A}/M$ is identical to the corresponding argument for congruences given in the proof of Theorem 8.6 (with Θ replaced by M). $\square$

$$\begin{tikzcd}
\mathfrak{A} \arrow[r, "\varphi"] \arrow[d, "\text{quotient homomorphism}"'] & \mathfrak{B} \\
\mathfrak{A}/M \arrow[ur, dashed, "\psi"'] &
\end{tikzcd}$$

Fig. 8.1 Diagram of the First Isomorphism Theorem.

Associated with the First Isomorphism Theorem is a cluster of related results of a universal algebraic kind, some of which we now proceed to state. The first concerns the connection between the quotients of a relation algebra $\mathfrak{A}$ and quotients of the subalgebras of $\mathfrak{A}$. In order to investigate this connection, it is necessary to study the relationship between ideals in $\mathfrak{A}$ and ideals in subalgebras of $\mathfrak{A}$. Every ideal in $\mathfrak{A}$ restricts to an ideal in each subalgebra of $\mathfrak{A}$, and every ideal in a subalgebra of $\mathfrak{A}$ is the restriction of some ideal in $\mathfrak{A}$.

Lemma 8.40. *Suppose $\mathfrak{B}$ is a subalgebra of a relation algebra $\mathfrak{A}$. If M is an ideal in $\mathfrak{A}$, then the intersection*

$$N = B \cap M \tag{i}$$

is an ideal in $\mathfrak{B}$. *Moreover*, *the ideal* N *is proper if and only if* M *is proper*. *Conversely*, *if* N *is an arbitrary ideal in* $\mathfrak{B}$, *then the ideal* M *generated by* N *in* $\mathfrak{A}$ *satisfies property* (i).

Proof. Assume first that M is an ideal in $\mathfrak{A}$, and let N be the set defined by (i). It is not difficult to verify that N satisfies the conditions in Definition 8.7 for being an ideal in $\mathfrak{B}$. For example, to verify conditions (iii) and (iv) in the definition (with N and $\mathfrak{B}$ in place of M and $\mathfrak{A}$ respectively), consider elements r in N and s in $\mathfrak{B}$. Clearly, r is in M and s in $\mathfrak{A}$, by (i) and the assumption that $\mathfrak{B}$ is a subalgebra of $\mathfrak{A}$, so the elements

$$r \cdot s, \qquad r \mathbin{;} s, \qquad s \mathbin{;} r \tag{1}$$

are all in M, by conditions (iii) and (iv) in Definition 8.7 applied to the ideal M in $\mathfrak{A}$. These elements also belong to $\mathfrak{B}$, because r and s are both in $\mathfrak{B}$, so the elements in (1) belong to the intersection $B \cap M$, which is N, by (i). Thus, conditions (iii) and (iv) holds for N. It is equally easy to check that conditions (i) and (ii) in Definition 8.7 are valid for N. The details are left as an exercise.

The unit element belongs to N if and only if it belongs to M, by the definition of N in (i) and the assumption that $\mathfrak{B}$ is a subalgebra of $\mathfrak{A}$ (and therefore has the same unit as $\mathfrak{A}$). It follows that the ideal N is proper if and only if M is proper, by the remarks at the beginning of Section 8.7.

To establish the final assertion of the lemma, suppose N is an arbitrary ideal in $\mathfrak{B}$, and M the ideal in $\mathfrak{A}$ that is generated by N. Obviously, N is included in the ideal $B \cap M$. To establish the reverse inclusion, consider an arbitrary element r in $B \cap M$. Since r is in M, there must be a finite subset Y of N such that r is below the ideal element

$$s = 1 \mathbin{;} (\textstyle\sum Y) \mathbin{;} 1,$$

by Theorem 8.12. The sum $\sum Y$ belongs to N, by Definition 8.7(ii) (applied to N and $\mathfrak{B}$), because N is an ideal and Y is a finite subset of N. Consequently, s belongs to N, by Definition 8.7(iv). It follows that r is in N, by Lemma 8.8(v) (with the roles of r and s reversed), because r belongs to $\mathfrak{B}$ and is below s. Thus, (i) holds. □

We continue with the assumption that $\mathfrak{B}$ is a subalgebra of $\mathfrak{A}$, and M an ideal in $\mathfrak{A}$. Take C to be the subuniverse of $\mathfrak{A}$ that is generated by

the union $B \cup M$. The quotient homomorphism from $\mathfrak{A}$ to $\mathfrak{A}/M$ maps the subuniverse C to the set

$$C/M = \{r/M : r \in C\},$$

so C/M is a subuniverse of $\mathfrak{A}/M$, by Lemma 7.4. Moreover, $B \cup M$ is a set of generators for C, by assumption, so

$$(B \cup M)/M = \{r/M : r \in B \cup M\}$$

is a set of generators for the subuniverse C/M, by Lemma 7.6 (with the subalgebra of $\mathfrak{A}$ whose universe is C and the subalgebra of $\mathfrak{A}/M$ whose universe is C/M in place of $\mathfrak{A}$ and $\mathfrak{A}/M$ respectively, and with the restriction of φ to the subalgebra with universe C in place of φ). For each element r in M, the coset r/M coincides with the coset $0/M$, since

$$r \equiv 0 \mod M.$$

Moreover, $0/M$ belongs to the set

$$B/M = \{r/M : r \in B\},$$

since 0 is in B, so

$$(B \cup M)/M = B/M.$$

This proves the following lemma.

Lemma 8.41. *Let $\mathfrak{B}$ be a subalgebra of a relation algebra $\mathfrak{A}$, and M an ideal in $\mathfrak{A}$. If C is the subuniverse of $\mathfrak{A}$ generated by the set $B \cup M$, then*

$$C/M = \{r/M : r \in C\}$$

is a subuniverse of $\mathfrak{A}/M$, and it is generated by the subset

$$B/M = \{r/M : r \in B\}.$$

Write $\mathfrak{C}$ for the subalgebra of $\mathfrak{A}$ with universe C. Obviously, M is also an ideal in $\mathfrak{C}$, so one may form the quotient $\mathfrak{C}/M$. What is the relationship between this quotient algebra and the subuniverse C/M of $\mathfrak{A}/M$ that was defined above? The notation suggests that the latter is the universe of the former, and this turns out to be the case, but it requires a proof. The reason is that, by definition, each coset in $\mathfrak{C}/M$ consists exclusively of elements from $\mathfrak{C}$. On the other hand, each coset in C/M is formed in $\mathfrak{A}/M$, and therefore might conceivably contain elements in $\mathfrak{A}$ that do not belong to $\mathfrak{C}$.

Lemma 8.42. *Let $\mathfrak{B}$ be a subalgebra of a relation algebra $\mathfrak{A}$, and M an ideal in $\mathfrak{A}$, and $\mathfrak{C}$ the subalgebra of $\mathfrak{A}$ generated by the set $B \cup M$. Then M is an ideal in $\mathfrak{C}$, and the quotient $\mathfrak{C}/M$ coincides with the subalgebra of $\mathfrak{A}/M$ whose universe is the set $C/M = \{r/M : r \in C\}$.*

Proof. Fix an element r in $\mathfrak{C}$. The coset of r in $\mathfrak{A}/M$ is defined to be the set

$$\{s \in A : s \equiv r \mod M\}, \tag{1}$$

while the coset of r in $\mathfrak{C}/M$ is defined to be the set

$$\{s \in C : s \equiv r \mod M\}. \tag{2}$$

The goal is to prove that these two sets are equal. Clearly, every element in (2) belongs to (1), because $\mathfrak{C}$ is a subalgebra of $\mathfrak{A}$. To establish the reverse inclusion, consider an arbitrary element s in (1). The definition in (1) implies that the element $s \ominus r$ must belong to the ideal M (see the remarks preceding Lemma 8.11), and therefore also to the subalgebra $\mathfrak{C}$, since M is a subset of this subalgebra. The element r also belongs to $\mathfrak{C}$, by assumption, so the symmetric difference of $s \ominus r$ and r belongs to $\mathfrak{C}$. Since

$$(s \ominus r) \ominus r = s \ominus (r \ominus r) = s \ominus 0 = s,$$

it follows that s belongs to C and therefore also to (2). Thus, the sets in (1) and (2) are equal, as claimed, so C/M is the universe of the algebra $\mathfrak{C}/M$.

It remains to check that the operations in $\mathfrak{C}/M$ coincide with the appropriate restrictions of the corresponding operations in $\mathfrak{A}/M$. Consider the case of the operation of relative multiplication. For elements r and s in $\mathfrak{C}$, the relative product of the cosets r/M and s/M in $\mathfrak{A}/M$ is defined by

$$(r/M) ; (s/M) = (r ; s)/M,$$

where the relative product $r ; s$ on the right is computed in $\mathfrak{A}$. The relative product of these two cosets in $\mathfrak{C}/M$ is defined by the same formula, except that the relative product $r ; s$ on the right is computed in $\mathfrak{C}$. Since $\mathfrak{C}$ is a subalgebra of $\mathfrak{A}$, the two computations yield the same result. A similar argument applies to the other operations. □

The next theorem is called the *Second Isomorphism Theorem*. It says that if M is an ideal in $\mathfrak{A}$, then the quotient of each subalgebra $\mathfrak{B}$ of $\mathfrak{A}$, modulo the ideal in $\mathfrak{B}$ that is induced by M, is isomorphic to a corresponding subalgebra of the quotient $\mathfrak{A}/M$.

Theorem 8.43. *Suppose $\mathfrak{B}$ is a subalgebra of a relation algebra $\mathfrak{A}$, and M an ideal in $\mathfrak{A}$, and $\mathfrak{C}$ the subalgebra of $\mathfrak{A}$ generated by $B \cup M$. The function φ defined by*

$$\varphi(r/(B \cap M)) = r/M$$

for each r in $\mathfrak{B}$ is an isomorphism from the quotient $\mathfrak{B}/(B \cap M)$ to the subalgebra $\mathfrak{C}/M$ of $\mathfrak{A}/M$.

Proof. Observe first that the intersection $B \cap M$ really is an ideal in $\mathfrak{B}$, by Lemma 8.40, so it makes sense to speak of the quotient of $\mathfrak{B}$ modulo this ideal. Consider elements r and s in $\mathfrak{B}$. The symmetric difference $r \ominus s$ also belongs to $\mathfrak{B}$, so $r \ominus s$ belongs to the ideal $B \cap M$ just in case it belongs to the ideal M. Consequently,

$$r \equiv s \mod B \cap M \qquad \text{if and only if} \qquad r \equiv s \mod M,$$

or, equivalently,

$$r/(B \cap M) = s/(B \cap M) \qquad \text{if and only if} \qquad r/M = s/M.$$

The function φ from $\mathfrak{B}/(B \cap M)$ to $\mathfrak{A}/M$ that is defined by

$$\varphi(r/(B \cap M)) = r/M$$

for all elements r in $\mathfrak{B}$ is therefore well defined and one-to-one. It is easy to check that φ preserves the operations. As an example, consider the operation of relative multiplication. We have

$$\begin{aligned}\varphi((r/(B \cap M))\,;(s/(B \cap M))) &= \varphi((r\,;s)/(B \cap M)) = (r\,;s)/M \\ &= (r/M)\,;(s/M) = \varphi(r/(B \cap M))\,;\varphi(s/(B \cap M))\end{aligned}$$

for all elements r and s in $\mathfrak{B}$, by the definition of relative multiplication in $\mathfrak{B}/(B \cap M)$, the definition of φ, and the definition of relative multiplication in $\mathfrak{A}/M$. The proofs that φ preserves addition, complement, and converse, and maps the identity element in $\mathfrak{B}/(B \cap M)$ to the identity element in $\mathfrak{A}/M$ are similar. Thus, φ is a monomorphism.

To prove that φ maps the universe of the domain algebra $\mathfrak{B}/(B\cap M)$ onto the set C/M, observe first that the image of this universe under the monomorphism φ must be a subuniverse of $\mathfrak{A}/M$, by Lemma 7.4. This image set—call it D—is determined by

$$\begin{aligned} D = \varphi(B/(B \cap M)) = \{\varphi(r/(B \cap M)) : r \in B\} \\ = \{r/M : r \in B\} = B/M. \end{aligned}$$

Since D is a subuniverse of $\mathfrak{A}/M$, and B/M is a set of generators for the subuniverse C/M, by Lemma 8.41, it follows that the two subuniverses must be equal. Apply Lemma 8.42 to conclude that φ maps $\mathfrak{B}/(B\cap M)$ isomorphically to $\mathfrak{C}/M$. □

Corollary 8.44. *Let $\mathfrak{B}$ be a subalgebra of a relation algebra $\mathfrak{A}$, and M an ideal in $\mathfrak{A}$. The function φ defined in Theorem 8.43 is an isomorphism from $\mathfrak{B}/(B \cap M)$ to $\mathfrak{A}/M$ if and only if the set $B \cup M$ generates $\mathfrak{A}$.*

Another consequence of the Second Isomorphism Theorem is that every quotient of a subalgebra of a relation algebra $\mathfrak{A}$ is isomorphic to a subalgebra of the corresponding quotient of $\mathfrak{A}$.

Corollary 8.45. *Suppose $\mathfrak{B}$ is a subalgebra of a relation algebra $\mathfrak{A}$, and N an arbitrary ideal in $\mathfrak{B}$. If M is the ideal generated by N in $\mathfrak{A}$, then the quotient $\mathfrak{B}/N$ is isomorphic to a subalgebra of the quotient $\mathfrak{A}/M$ via the function that maps r/N to r/M for each r in $\mathfrak{B}$.*

Proof. It was shown in the final part of Lemma 8.40 that if M is the ideal generated by N in $\mathfrak{A}$, then

$$N = B \cap M.$$

Consequently, we may replace $B\cap M$ by N in the Second Isomorphism Theorem to conclude that the function mapping r/N to r/M for each r in $\mathfrak{B}$ is a monomorphism from $\mathfrak{B}/N$ to $\mathfrak{A}/M$. □

As an application of some of the results we have seen so far in this section, we prove the following *Homomorphism Extension Theorem.*

Theorem 8.46. *Let $\mathfrak{B}$ be a subalgebra of a relation algebra $\mathfrak{A}$. Every homomorphism φ from $\mathfrak{B}$ onto an algebra $\mathfrak{C}$ can be extended to a homomorphism from $\mathfrak{A}$ onto an algebra $\mathfrak{D}$ that includes $\mathfrak{C}$ as a subalgebra. If φ is a monomorphism, then so is the extension.*

Proof. Consider a homomorphism φ on $\mathfrak{B}$. Let $\mathfrak{C}$ be the image algebra of $\mathfrak{B}$ under φ, and N the kernel of φ. The quotient $\mathfrak{B}/N$ is isomorphic to $\mathfrak{C}$ via the function δ defined by

$$\delta(r/N) = \varphi(r) \tag{1}$$

for all r in $\mathfrak{B}$, by the First Isomorphism Theorem 8.39 (see Figure 8.2). Let M be the ideal in $\mathfrak{A}$ generated by N. The quotient $\mathfrak{B}/N$ is embeddable into the quotient $\mathfrak{A}/M$ via the monomorphism ϱ defined by

$$\varrho(r/N) = r/M \tag{2}$$

for each element r in $\mathfrak{B}$, by Corollary 8.45. Consequently, the composition $\varrho \circ \delta^{-1}$ is a monomorphism from $\mathfrak{C}$ into $\mathfrak{A}/M$ (see Figure 8.2). Apply the Exchange Principle (Theorem 7.15) to obtain a relation algebra $\mathfrak{D}$ that includes $\mathfrak{C}$ as a subalgebra and that is isomorphic to $\mathfrak{A}/M$ via a mapping χ that extends $\varrho \circ \delta^{-1}$. Observe that the inverse function χ^{-1} is an isomorphism from $\mathfrak{A}/M$ to $\mathfrak{D}$ that extends the mapping $\delta \circ \varrho^{-1}$.

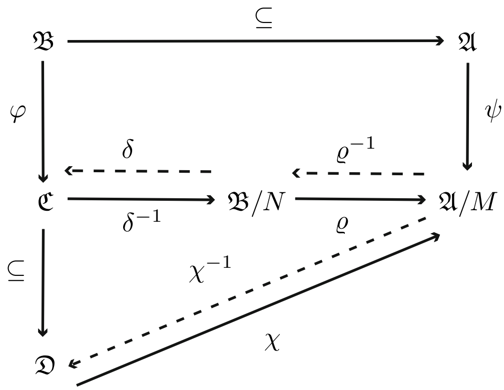


Fig. 8.2 Diagram of the Homomorphism Extension Theorem.

Let ψ be the quotient homomorphism from $\mathfrak{A}$ onto $\mathfrak{A}/M$ that is defined by

$$\psi(r) = r/M \tag{3}$$

for all r in $\mathfrak{A}$. The composition

$$\vartheta = \chi^{-1} \circ \psi \tag{4}$$

is a homomorphism from $\mathfrak{A}$ onto $\mathfrak{D}$ (see Figure 8.2), and for each element r in $\mathfrak{B}$, we have

$$\begin{aligned}\vartheta(r) = (\chi^{-1} \circ \psi)(r) = \chi^{-1}(\psi(r)) = \chi^{-1}(r/M)\\ = (\delta \circ \varrho^{-1})(r/M) = \delta(\varrho^{-1}(r/M)) = \delta(r/N) = \varphi(r),\end{aligned}$$

by (4), (3), the fact that χ^{-1} extends $\delta \circ \varrho^{-1}$, (2), and (1). Thus, ϑ agrees with the homomorphism φ on elements r in $\mathfrak{B}$, so ϑ is an extension of φ.

The kernel of φ is the ideal N in $\mathfrak{B}$, by assumption. In view of (4), the kernel of ϑ must be the ideal M in $\mathfrak{A}$ that is generated by N, because the kernel of ψ is M, by Theorem 8.38, and χ^{-1} is an isomorphism. If φ is one-to-one, then its kernel N is the trivial ideal $\{0\}$, by Lemma 8.37. Consequently, the ideal M generated in $\mathfrak{A}$ by N is also the trivial ideal, and therefore ϑ is one-to-one, by Lemma 8.37. □

Next, we study the relationship between the ideals in a relation algebra $\mathfrak{A}$ and the ideals in a quotient of $\mathfrak{A}$. Suppose M is a proper ideal in $\mathfrak{A}$. Write $[M, A]$ for the set, or *interval*, of ideals N in $\mathfrak{A}$ such that $M \subseteq N \subseteq A$. This interval forms a sublattice, and in fact a complete sublattice, of the lattice of ideals in $\mathfrak{A}$. It turns out that this sublattice is isomorphic to the lattice of ideals of the quotient $\mathfrak{A}/M$ in a natural way.

Write $\mathfrak{B} = \mathfrak{A}/M$, and let φ be the quotient homomorphism from $\mathfrak{A}$ onto $\mathfrak{B}$. This homomorphism associates with each ideal N in the interval $[M, A]$ an ideal in $\mathfrak{B}$, namely the image ideal

$$L = \varphi(N) = \{\varphi(r) : r \in N\} = \{r/M : r \in N\},$$

by the second assertion in Lemma 8.11. A common notation for this image ideal is N/M. Conclusion: the correspondence

$$N \longmapsto \varphi(N) = N/M$$

induced by φ is a mapping from the sublattice $[M, A]$ into the lattice of ideals in $\mathfrak{B}$.

Similarly, using the first assertion in Lemma 8.11, we see that if L is an arbitrary ideal in $\mathfrak{B}$, then its inverse image

$$N = \varphi^{-1}(L) = \{r \in \mathfrak{A} : \varphi(r) \in L\}$$

is an ideal in $\mathfrak{A}$. The ideal N includes M, because L contains the zero element of $\mathfrak{B}$, and M is the inverse image under φ of zero, by Theorem 8.38. Consequently, N is an ideal in the sublattice $[M, A]$.

It is not too difficult to check that

$$\varphi(\varphi^{-1}(L)) = L \qquad \text{and} \qquad \varphi^{-1}(\varphi(N)) = N$$

for every ideal L in $\mathfrak{B}$ and every ideal N in $\mathfrak{A}$. We begin with the proof of the first equation. Assume that r/M belongs to the ideal L. Since $\varphi(r) = r/M$, the element r must belong to $\varphi^{-1}(L)$, by the definition of the inverse image of a set under a function. Consequently, $\varphi(r)$ must belong to the image set $\varphi(\varphi^{-1}(L))$, by the definition of the image of a set under a function. In other words, r/M is in $\varphi(\varphi^{-1}(L))$. This proves that L is included in $\varphi(\varphi^{-1}(L))$. The the reverse inclusion follows by the definition of the inverse image set. According to this definition, the inverse image $\varphi^{-1}(L)$ consists of those elements in $\mathfrak{A}$ that are mapped by φ to elements in L. Obviously, the image under φ of each element in this inverse image belongs to L, so $\varphi(\varphi^{-1}(L))$ is included in L.

For the proof of the second equation, observe that every element r in N belongs to the inverse image $\varphi^{-1}(\varphi(r))$, and therefore to inverse image $\varphi^{-1}(\varphi(N))$, by the definition of the inverse image of a set under a function. Thus, N is included in $\varphi^{-1}(\varphi(N))$. To establish the reverse inclusion, consider an arbitrary element r in $\varphi^{-1}(\varphi(N))$. The image $\varphi(r)$ of this element belongs to $\varphi(N)$, by the definition of the inverse image of a set under a function, so there must be an element s in N such that $\varphi(r) = \varphi(s)$. It follows that

$$\varphi(r \ominus s) = \varphi(r) \ominus \varphi(s) = \varphi(r) \ominus \varphi(r) = 0,$$

by the homomorphism properties of φ and the definition of symmetric difference. The element $r \ominus s$ therefore belongs to the kernel of φ, which is M. The ideal N includes M, by assumption, so N contains the element $r \ominus s$ as well. Since N also contains s, and since ideals are closed under the operation of symmetric difference, by condition (vii) in Lemma 8.8, the element $(r \ominus s) \ominus s$ must belong to N. This element is just r, so r belongs to N, as was to be shown.

The preceding observations imply that the correspondence induced by φ maps the interval $[M, A]$ bijectively to the lattice of ideals in $\mathfrak{B}$. Indeed, if L is an ideal in $\mathfrak{B}$, then $N = \varphi^{-1}(L)$ is an ideal in $\mathfrak{A}$, and

$$\varphi(N) = \varphi(\varphi^{-1}(L)) = L,$$

so the induced correspondence is onto. If N_1 and N_2 are ideals in $[M, A]$ such that

$$\varphi(N_1) = \varphi(N_2),$$

then

$$N_1 = \varphi^{-1}(\varphi(N_1)) = \varphi^{-1}(\varphi(N_2)) = N_2,$$

so the induced correspondence is one-to-one.

A similar argument shows that the induced correspondence preserves the lattice partial order of inclusion. If $N_1 \subseteq N_2$, then obviously $\varphi(N_1) \subseteq \varphi(N_2)$. If, conversely, the latter inclusion holds, then

$$\varphi^{-1}(\varphi(N_1)) \subseteq \varphi^{-1}(\varphi(N_2)),$$

and therefore $N_1 \subseteq N_2$. It follows that the induced correspondence is a lattice isomorphism. The following result, called the *Correspondence Theorem*, has been proved.

Theorem 8.47. *For every ideal M in a relation algebra $\mathfrak{A}$, the correspondence $N \longmapsto N/M$ is an isomorphism from the sublattice of ideals in $\mathfrak{A}$ that include M to the lattice of ideals in $\mathfrak{A}/M$.*

The relationship between the ideals in a quotient $\mathfrak{A}/M$ and the ideals in $\mathfrak{A}$ that extend M goes beyond what is expressed in the Correspondence Theorem. Quotients of $\mathfrak{A}/M$ by quotient ideals N/M are in fact isomorphic to quotients of $\mathfrak{A}$. It is therefore unnecessary to consider quotients of quotient relation algebras, quotients of quotients of quotient relation algebras, and so on. Each such quotient essentially reduces to a quotient of the original relation algebra. A precise formulation of this fact is contained in the following theorem, known as the *Third Isomorphism Theorem*.

Theorem 8.48. *Let M and N be ideals in a relation algebra $\mathfrak{A}$, with $M \subseteq N$. The quotient of $\mathfrak{A}/M$ by the ideal N/M is isomorphic to the quotient $\mathfrak{A}/N$ via the mapping*

$$(r/M)/(N/M) \longmapsto r/N.$$

Proof. Write

$$\mathfrak{B} = \mathfrak{A}/M \qquad \text{and} \qquad \mathfrak{C} = \mathfrak{B}/(N/M) = (\mathfrak{A}/M)/(N/M).$$

The quotient mapping φ from $\mathfrak{A}$ onto $\mathfrak{B}$, and the quotient mapping ψ from $\mathfrak{B}$ onto $\mathfrak{C}$, are both epimorphisms, so the composition $\vartheta = \psi \circ \varphi$ is an epimorphism from $\mathfrak{A}$ onto $\mathfrak{C}$. The kernel of ϑ is N, as can be verified in two steps: the kernel of ψ is the ideal N/M, by Theorem 8.38; and the set of elements in $\mathfrak{A}$ that are mapped into N/M by φ is just

$$\varphi^{-1}(N/M) = \varphi^{-1}(\varphi(N)) = N.$$

The First Isomorphism Theorem applied to the epimorphism ϑ says

$$\begin{tikzcd}
\mathfrak{A} \arrow[d, "\varphi"'] \arrow[dr, "\vartheta"] & \mathfrak{A}/N \arrow[d, shift right, "\varrho"'] \\
(\mathfrak{A}/M) \arrow[r, "\psi"] & (\mathfrak{A}/M)/(N/M) \arrow[u, dashed, shift right, "\varrho^{-1}"']
\end{tikzcd}$$

Fig. 8.3 Diagram of the Third Isomorphism Theorem.

that the quotient $\mathfrak{A}/N$ is isomorphic to $\mathfrak{C}$ via the function ϱ that maps each coset r/N to $\vartheta(r)$ (see Figure 8.3). The proof is completed by observing that

$$\varrho(r/N) = \vartheta(r) = \psi(\varphi(r)) = \psi(r/M) = (r/M)/(N/M),$$

so the inverse of the isomorphism ϱ is the mapping in the conclusion of the theorem. $\square$

8.12 Filters

As we have seen, congruences are determined by the congruence class of a single element, namely 0, and the congruence class of 0 can be characterized abstractly by four conditions, namely the conditions in the definition of an ideal. It is natural to ask whether the congruence class of some other element, for example, the congruence class of 1, could also be used for the same purpose. Consider a congruence Θ on a relation algebra, and let M be the congruence class of 0, and N the congruence class of 1. An element r belongs to M if and only if its complement $-r$ belongs to N, because

$$r \equiv 0 \mod \Theta \qquad \text{if and only if} \qquad -r \equiv 1 \mod \Theta,$$

by the preservation properties of congruences and the Boolean law of double negation, $-(-r) = r$. Thus,

$$N = \{-r : r \in M\}.$$

This simple observation implies that every definition or result about congruence classes of 0—that is to say, about ideals—can be dualized to a definition or result about congruence classes of 1 just by "forming the complement" in an appropriate fashion of the definition or result. We sketch this development below, leaving most of the details as exercises. Let's start with the dual of the concept of an ideal.

Definition 8.49. A *filter* in a relation algebra $\mathfrak{A}$ is a subset N of the universe with the following properties.

(i) 1 is in N.
(ii) If r and s are in N, then $r \cdot s$ is in N.
(iii) If r is in N and s in $\mathfrak{A}$, then $r + s$ is in N.
(iv) If r is in N and s in $\mathfrak{A}$, then $r \mathbin{+\!\!\!,} s$ and $s \mathbin{+\!\!\!,} r$ are in N. □

Conditions (i)–(iii) say that N is a *Boolean filter* (see, for example, [38]). Consequently, a relation algebraic filter is a Boolean filter that is closed under relative addition by arbitrary elements from the relation algebra, that is to say, it is a Boolean filter in which condition (iv) holds. Just as in the case of ideals, each of conditions (i)–(iv) has a useful equivalent formulation. To formulate one of these equivalent conditions, it is necessary to introduce the (Boolean) dual of the operation of symmetric difference; this dual is the binary operation $\Leftrightarrow$ that is defined by

$$r \Leftrightarrow s = (-r + s) \cdot (-s + r)$$

for all elements r and s.

Lemma 8.50. *Condition* (iii) *is equivalent to the condition*:

(v) *If r is in N and $r \le s$, then s is in N.*

Under the assumption of condition (iii), *the following further equivalences hold. Condition* (i) *is equivalent to the condition*:

(vi) *N is not empty.*

Condition (ii) *is equivalent to the condition*:

(vii) *If* r *and* s *are in* N, *then* $r \Leftrightarrow s$ *is in* N.

Condition (iv) *is equivalent to the conjunction of the two conditions*:

(viii) *If* r *is in* N, *then* $r^{\smile}$ *is in* N.
(ix) *If* r *is in* N *and* s *in* $\mathfrak{A}$, *then* $r \dagger s$ *is in* N.

The *cokernel* of a congruence Θ on a relation algebra $\mathfrak{A}$ is defined to be the set of elements that are congruent to 1 modulo Θ. The cokernel of every congruence on $\mathfrak{A}$ is a filter in $\mathfrak{A}$, and conversely, every filter in $\mathfrak{A}$ uniquely determines a congruence Θ on $\mathfrak{A}$ of which it is the cokernel. In fact, if N is a filter in $\mathfrak{A}$, and if Θ is the relation on the universe of $\mathfrak{A}$ that is defined by

$$r \equiv s \mod \Theta \qquad \text{if and only if} \qquad r \Leftrightarrow s \in N,$$

then Θ is a congruence on $\mathfrak{A}$, and N is the cokernel of Θ. Moreover, Θ is the unique congruence on $\mathfrak{A}$ with cokernel N.

One consequence of this observation is that a filter is closed under relative multiplication: if r and s belong to N, then $r\,;s$ is also in N. Another consequence is that every congruence class of Θ can be computed directly from the cokernel N: for each element r, the congruence class r/Θ coincides with the *cokernel coset*

$$r \Leftrightarrow N = \{r \Leftrightarrow s : s \in N\}.$$

The definitions of the operations and distinguished elements of the quotient algebra $\mathfrak{A}/\Theta$ can all be expressed in terms of the cokernel cosets of the filter N. Consequently, in the study of relation algebra, congruences can equally well be replaced by filters instead of ideals, and congruence classes can be replaced by cokernel cosets instead of cosets. The notion of the quotient of a relation algebra by a congruence can be replace by the notion of the quotient of a relation algebra by a filter, and in fact the two notions actually coincide. The quotient homomorphism from $\mathfrak{A}$ to the quotient $\mathfrak{A}/N$ may be defined as the function that maps each element r to its cokernel coset $r \Leftrightarrow N$. The *cokernel* of this homomorphism is, by definition, the set of elements that are mapped to the unit element $1/N$, which is just N. All of these observations can be proved by dualizing the proofs of the analogous observations about ideals. Similar arguments show that the image of a filter under epimorphism is again a filter, and the inverse image of a filter under a homomorphism is again a filter.

Every relation algebra $\mathfrak{A}$ has a smallest filter, namely the set $\{1\}$. This is called the *trivial filter*; all other filters are called *non-trivial*. There is also a largest filter in $\mathfrak{A}$, namely the universe A. This is called the *improper filter*; all other filters are called *proper*. A filter is proper if and only if it does not contain the zero element 0.

The intersection of an arbitrary system of filters in a relation algebra $\mathfrak{A}$ is again a filter. If X is an arbitrary subset of $\mathfrak{A}$, then the filter *generated* by X is defined to be the intersection of the system of all filters in $\mathfrak{A}$ that include X as a subset. That intersection is the smallest filter that includes X. In analogy with Theorem 8.12, one can prove that an element r belongs to the filter generated by a set X if and only if there is a finite subset Y of X such that

$$0 \mathbin{+\!\!\!\!,} \left(\prod Y\right) \mathbin{+\!\!\!\!,} 0 \leq r.$$

A filter is said to be *finitely generated* if it is generated by some finite set, and *principal* if it is generated by a single element. If N is the principal filter generated by an element r, then

$$N = \{s \in A : 0 \mathbin{+\!\!\!\!,} r \mathbin{+\!\!\!\!,} 0 \leq s\}.$$

For this reason, elements of the form $0 \mathbin{+\!\!\!\!,} r \mathbin{+\!\!\!\!,} 0$ might be called *filter elements*. Actually, Corollary 4.31 and its first dual imply that every filter element is an ideal element, and conversely, every ideal element is a filter element. Consequently, there is no need to introduce new terminology; the term ideal element is applicable in both cases. Every principal filter has a smallest element r, and r is an ideal element; the filter consists of all those elements s that are above r. The trivial filter $\{1\}$ and the improper filter A are both principal; the former is generated by the ideal element 1 and the latter by the ideal element 0. Every finitely generated filter is principal.

The set of all filters in a relation algebra $\mathfrak{A}$ is partially ordered by the relation of set-theoretic inclusion, and under this partial order it becomes a complete, compactly generated, distributive lattice. The join and meet of two filters M and N in this lattice are respectively just the complex product and sum of the two filters:

$$M \vee N = \{r \cdot s : r \in M \text{ and } s \in N\}$$

and

$$M \wedge N = \{r + s : r \in M \text{ and } s \in N\}.$$

The compact elements in the lattice are the finitely generated filters, which coincide with the principal filters. The meet of a system of filters is the intersection of the system, and the join of the system is the filter generated by the union of the system. For non-empty directed systems of filters, the supremum of the system is the union of the filters in the system. Every filter N is the union of a directed system of principal filters. In fact, if r and s are ideal elements in N, then $r \cdot s$ is also an ideal element in N, and the principal filters generated by r and by s are both included in the principal filter generated by $r \cdot s$.

If N is a filter in $\mathfrak{A}$, then the intersection of N with the Boolean algebra B of ideal elements in $\mathfrak{A}$, that is to say, the set

$$B_N = B \cap N,$$

is a Boolean filter in B. Conversely, if L is a Boolean filter in B, then the set

$$A_L = \{r \in A : 0 \mathbin{+\!\!\!\!,} r \mathbin{+\!\!\!\!,} 0 \in L\} = \{r \in A : s \leq r \text{ for some } s \in L\}$$

is a filter in $\mathfrak{A}$. The equations

$$A_{B_N} = N \qquad \text{and} \qquad B_{A_L} = L$$

are easy to prove, and they imply that the function mapping each filter N in $\mathfrak{A}$ to the Boolean filter $B \cap N$ in B is a bijection, and in fact a lattice isomorphism, from the lattice of filters in $\mathfrak{A}$ to the lattice of Boolean filters in the Boolean algebra B. This isomorphism maps the set of principal filters in $\mathfrak{A}$ bijectively to the set of principal Boolean filters in B.

As the preceding discussion makes clear, the relation between filters and ideals is a very close one, and in fact, filters and ideals come in dual pairs: if M is an ideal in a relation algebra $\mathfrak{A}$, then the set

$$N = \{-r : r \in M\}$$

is a filter in $\mathfrak{A}$, called the *dual filter* of M; and in reverse, if N is a filter in $\mathfrak{A}$, then the set

$$M = \{-r : r \in N\}$$

is an ideal in $\mathfrak{A}$, called the *dual ideal* of N. The dual ideal of the dual filter of an ideal M is obviously just M, by the Boolean law of double

negation, and the dual filter of the dual ideal of a filter N is just N. Consequently, the function φ that maps each ideal to its dual filter is a bijection from the lattice of ideals in $\mathfrak{A}$ to the lattice of filters in $\mathfrak{A}$. If M_1 and M_2 are ideals with dual filters N_1 and N_2 respectively, then

$$M_1 \subseteq M_2 \qquad \text{if and only if} \qquad N_1 \subseteq N_2,$$

so the bijection φ is actually a lattice isomorphism. Conclusion: the lattice of ideals in $\mathfrak{A}$ is isomorphic to the lattice of filters in $\mathfrak{A}$ via the function that maps each ideal to its dual filter.

8.13 Historical remarks

Ideals have been studied in one form or another since the time of Dedekind (see [27]). Congruences are used in place of ideals in the general study of algebras and quotients of algebras, because there is no notion of ideal that applies to all algebras. Lemma 8.2 and Theorem 8.3 were given by Tarski in his lectures [112], but the corresponding result for the lattice of normal subgroups of a group is of much earlier origins (see [11]). The Homomorphism Theorem, and the three Isomorphism Theorems are well-known results about arbitrary algebras that, in their applications to groups, rings, and modules, date back to the works of Dedekind, Noether, and van der Waerden. The Correspondence Theorem occurs in [39] in a form applicable to arbitrary algebras, but the version of the theorem that applies to the lattice of normal subgroups of a group is of earlier origins.

The study of ideals in the context of relation algebras was initiated by Tarski. The definition of an ideal in Definition 8.7, and the characterization of condition (iv) in Lemma 8.8, are contained in [105] and [112]; the definition appears explicitly in [55]. The observation in Corollary 8.10 is due to Givant, as is Lemma 8.28 (see [34]). The important Theorems 8.12 and 8.26 (the Lattice of Ideals Theorem) are due to Tarski and are contained in [105] and [112], as are the formulations of the Homomorphism Theorem and the First Isomorphism Theorem in the context of relation algebras. Exercise 8.51 and Corollary 8.13 occur in [105], and Corollary 8.14 occurs in [112]. The characterizations of the join and meet of two ideals that are given in Lemma 8.17 and Corollary 8.18 are generalizations, due to Givant, of known results about ideals in Boolean algebras (see, for example, [38]), and the

strengthening of Theorem 8.3 that is given in Theorem 8.22 (namely, that the lattice is distributive, and that the join and meet of two ideals are equal to their complex sum and product respectively) is also due to Givant.

The characterizations of maximal ideals in Lemma 8.29, and the form of the Maximal Ideal Theorem which says that every proper ideal is included in a maximal ideal, are both due to Tarski and are contained in [105] and [112], as is also a version of Lemma 8.32. The stronger version of the Maximal Ideal Theorem that is given in Theorem 8.30 is discussed in [112]. These results, as well as several of the remaining results in Section 8.10, are implied by the Lattice of Ideals Theorem, because they are relation algebraic versions of theorems that hold for Boolean algebras. The characterization in Lemma 8.33 of maximal non-principal ideals, and the characterization in Theorem 8.34 of relation algebras possessing such ideals, are due to Givant. The formulation and proof of the Homomorphism Extension Theorem 8.46 are also due to Givant. This theorem is actually valid in the context of varieties of algebras with a discriminator term (see, for example, Exercise 8.83).

Tarski was aware that the entire discussion of ideals could equivalently be replaced by a corresponding discussion of filters, and he touches upon this matter in [112].

The notion of an ideal in a Boolean algebra with normal operators, which is discussed in Exercise 8.78, was first given by Ildikó Sain [93], Proposition 7.4, for the case of unary operators. The general definition used here was given by Andréka, Givant, Mikulás, Németi, and Simon [4], Lemma 2.4. The generalization in Exercise 8.80 of some of the main results about ideals, and the laws in Exercise 8.79, are from [4]

Exercises

8.1. Prove that the universal relation $A \times A$ and identity relation id_A are always congruences on a relation algebra $\mathfrak{A}$, and in fact they are the largest and the smallest congruences respectively.

8.2. Prove that the union of a non-empty directed system of congruences on a relation algebra $\mathfrak{A}$ is again a congruence on $\mathfrak{A}$. Conclude that the union of a non-empty chain of congruences on $\mathfrak{A}$ is a congruence on $\mathfrak{A}$.

8.3. Suppose Θ is a congruence on a relation algebra $\mathfrak{A}$ that is generated by a set X, and write Θ_Y for the congruence on $\mathfrak{A}$ that is generated by a subset Y of X. Prove that the system of congruences

$$(\Theta_Y : Y \subseteq X \text{ and } Y \text{ is finite})$$

is directed and its union is Θ. Conclude that every congruence on $\mathfrak{A}$ is the union of a directed system of finitely generated congruences.

8.4. Prove that every finitely generated congruence on a relation algebra $\mathfrak{A}$ is compact in the lattice of congruences on $\mathfrak{A}$. Conclude that the lattice is compactly generated.

8.5. Prove for an arbitrary equivalence relation Θ on a set A that

$$r/\Theta = s/\Theta \qquad \text{if and only if} \qquad r \equiv s \mod \Theta$$

for all r and s in A. Conclude that any two equivalence classes of Θ are either equal or disjoint.

8.6. For a congruence Θ on a relation algebra $\mathfrak{A}$, show that the operations of addition, complement, and converse that are defined on the set of congruence classes of Θ in Section 8.5 are well defined.

8.7. Show directly that Axioms (R5)–(R10) hold in the quotient of a relation algebra modulo a congruence.

8.8. Show that the quotient homomorphism mapping a relation algebra $\mathfrak{A}$ to a quotient algebra $\mathfrak{A}/\Theta$ is onto and preserves the operations of addition, complement, and converse.

8.9. For an arbitrary homomorphism φ from a relation algebra $\mathfrak{A}$ into a relation algebra $\mathfrak{B}$, prove that the relation Θ on $\mathfrak{A}$ defined by

$$(r, s) \in \Theta \qquad \text{if and only if} \qquad \varphi(r) = \varphi(s)$$

is an equivalence relation on the universe of $\mathfrak{A}$, and that Θ preserves the operations of addition, complement, and converse. Conclude that Θ is a congruence on $\mathfrak{A}$.

8.10. Prove that the bijection ψ in the proof of Theorem 8.6 preserves the operation of addition.

8.11. Verify that in a relation algebra $\mathfrak{A}$, the sets A and $\{0\}$ are ideals, and in fact they are respectively the largest and the smallest ideals in $\mathfrak{A}$.

8.12. Prove that the following conditions on an ideal M are equivalent: (1) M is improper; (2) there is an element r such that r and $-r$ are both in M; (3) 1 is in M.

8.13. A subset X of a relation algebra is said to have the *finite join property* if, for any finite subset Y of X, the ideal element $1 ; (\sum Y) ; 1$ is different from 1. Prove that the ideal generated by a set X is proper if and only if X has the finite join property.

8.14. For any two elements r and s in a relation algebra, prove that the sum $r + s$ belongs to an ideal M if and only if both r and s belong to M.

8.15. Prove the first assertion of Lemma 8.11. Show that the second assertion may fail if the homomorphism φ does not map $\mathfrak{A}$ onto $\mathfrak{B}$.

8.16. Suppose φ is an epimorphim from $\mathfrak{A}$ to $\mathfrak{B}$. If a set X generates an ideal M in $\mathfrak{A}$, prove that the image set $\varphi(X)$ generates the image ideal $\varphi(M)$ in $\mathfrak{B}$.

8.17. Suppose φ is an epimorphim from $\mathfrak{A}$ to $\mathfrak{B}$. If a set Y generates an ideal N in $\mathfrak{B}$, is it true that the inverse image set

$$\varphi^{-1}(Y) = \{r \in A : \varphi(r) \in Y\}$$

generates the inverse image ideal $\varphi^{-1}(N)$ in $\mathfrak{A}$?

8.18. Suppose φ is an epimorphim from $\mathfrak{A}$ to $\mathfrak{B}$. If an ideal N in $\mathfrak{B}$ is finitely generated, is it true that the inverse image ideal

$$\varphi^{-1}(N) = \{r \in A : \varphi(r) \in N\}$$

is finitely generated?

8.19. Verify that the intersection of a system of ideals satisfies conditions (i)–(iii) of Definition 8.7.

8.20. Let M be an ideal in a relation algebra $\mathfrak{A}$. The *annihilator* of M is defined to be the set of elements r in $\mathfrak{A}$ such that $r \cdot s = 0$ for all s in M. Prove that the annihilator of an ideal is an ideal.

8.21. Prove that the intersection of two ideals M and N in a relation algebra is the trivial ideal if and only if N is included in the annihilator of M (see Exercise 8.20). Conclude that the annihilator of M is the largest ideal with the property that its intersection with M is the trivial ideal.

8.22. Call a subset of a relation algebra $\mathfrak{A}$ *quasi-dense* in $\mathfrak{A}$ if every non-zero ideal element in $\mathfrak{A}$ is above a non-zero element of the subset. Prove that an ideal M in $\mathfrak{A}$ is quasi-dense if and only if M has a non-trivial intersection with every non-trivial ideal in $\mathfrak{A}$. Conclude that M is quasi-dense if and only if its annihilator (see Exercise 8.20) is the trivial ideal.

8.23. Complete the proof of Lemma 8.40 by showing that the set N defined in (i) satisfies conditions (i) and (ii) in Definition 8.7.

8.24. Suppose $\mathfrak{B}$ is a subalgebra of a relation algebra $\mathfrak{A}$, and M is an ideal in $\mathfrak{A}$. If M is a subset of the universe of $\mathfrak{B}$, prove that M must be an ideal in $\mathfrak{B}$.

8.25. Prove that if an ideal M in a relation algebra $\mathfrak{A}$ is countably generated (generate by a countable set), then there must be a (countable) ascending chain

$$r_1 \le r_2 \le \cdots \le r_n \le \dots$$

of ideal elements in M such that an element s in $\mathfrak{A}$ belongs to M if and only if $s \le r_n$ for some positive integer n.

8.26. Prove Corollary 8.18.

8.27. Let $(M_i : i \in I)$ be an arbitrary system of ideals in a relation algebra. Define a *finite sum* of elements in this system to be an element of the form $\sum_{i\in J} r_i$, where J is some finite subset of I, and r_i belongs to the ideal M_i for each i in J. Prove that the join $\bigvee_{i\in I} M_i$ in the lattice of ideals is the set of all finite sums of elements in the given system of ideals.

8.28. Give an example to show that the meet of an infinite system of principal ideals need not be a principal ideal. Why does this not contradict Lemma 8.19(ii)?

8.29. Prove that the implication from right to left in Lemma 8.19(i) may fail.

8.30. Prove by a direct argument that the ideals in a relation algebra satisfy the distributive law

$$L \wedge (M \vee N) = (L \wedge M) \vee (L \wedge N).$$

8.31. Suppose K is a Boolean ideal in the Boolean algebra B of ideal elements in a relation algebra $\mathfrak{A}$. Prove that the set

$$A_K = \{r \in A : 1 \mathbin{;} r \mathbin{;} 1 \in K\} = \{r \in A : r \leq s \text{ for some } s \in B\}$$

is an ideal in $\mathfrak{A}$.

8.32. Prove that the ideal generated by the set of atoms in a relation algebra $\mathfrak{A}$ is proper if the Boolean algebra of ideal elements in $\mathfrak{A}$ is infinite. What about the converse?

8.33. Prove that in a Boolean algebra, the intersection of an ideal with a subalgebra is always an ideal in the subalgebra.

8.34. Let B be the Boolean algebra of ideal elements in a relation algebra $\mathfrak{A}$. If one starts with a Boolean ideal K in B, forms the relation algebraic ideal A_K in $\mathfrak{A}$, and then forms the Boolean ideal B_{A_K} in B, prove that the result is the original Boolean ideal K (see the remarks after Corollary 8.25).

8.35. Construct an example of a non-degenerate atomless relation algebra with two ideal elements, 0 and 1. Conclude that a non-degenerate atomless relation algebra can have an atomic Boolean algebra of ideal elements.

8.36. Use Theorem 6.18 to give another proof of the second assertion of Lemma 8.28, which says that if a relation algebra is atomic, then its Boolean algebra of ideal elements is also atomic.

8.37. Another version of the Maximal Ideal Theorem 8.31 says simply that every proper ideal is included in a maximal ideal. Prove that this version implies Theorem 8.31.

8.38. Fill in the details of the following sketch of an alternative proof of the theorem that every proper ideal in a relation algebra is included in a maximal ideal. Let M be a proper ideal in a relation algebra $\mathfrak{A}$. Enumerate the ideal elements of $\mathfrak{A}$ in a (possibly) transfinite sequence $(r_i : i < \alpha)$ indexed by the set of ordinal numbers less than

some ordinal α. Define a corresponding sequence $(M_i : i \leq \alpha)$ of proper ideals in $\mathfrak{A}$ with the following properties: (1) $M_0 = M$; (2) $M_i \subseteq M_j$ whenever $i \leq j \leq \alpha$; (3) either r_i or $-r_i$ is in M_{i+1} for each $i < \alpha$. The definition proceeds by induction on i. Put $M_0 = M$. For the induction step, consider an ordinal $k \leq \alpha$, and suppose that proper ideals M_i have been defined for every $i < k$ such that the sequence of ideals M_i for $i < k$ has properties (1)–(3) (with α replaced by k). When k is a successor ordinal, say $k = i + 1$, the definition of M_k splits into two cases. If either r_i or $-r_i$ is in M_i, put $M_k = M_i$. If neither of these elements is in M_i, define M_k to be the ideal generated by the set $M_i \cup \{r_i\}$. When k is a limit ordinal, defined M_k to be the union of the ideals M_i for $i < k$. The set M_α is the desired maximal ideal extending M.

8.39. Suppose $\mathfrak{B}$ is a subalgebra of a relation algebra $\mathfrak{A}$. If M is a maximal ideal in $\mathfrak{A}$, prove that $M \cap B$ is a maximal ideal in $\mathfrak{B}$.

8.40. Suppose φ is a homomorphism from $\mathfrak{A}$ to $\mathfrak{B}$. If N is a maximal ideal in $\mathfrak{B}$, prove that the inverse image of N under φ, that is to say, the set

$$M = \{r \in A : \varphi(r) \in N\},$$

is a maximal ideal in $\mathfrak{A}$.

8.41. If a subset X of a relation algebra has the finite join property (see Exercise 8.13), prove that X is included in a maximal ideal.

8.42. Suppose $\mathfrak{B}$ is a subalgebra of a relation algebra $\mathfrak{A}$. If $\mathfrak{A}$ contains an ideal element that is not in $\mathfrak{B}$, prove that there is a maximal ideal in $\mathfrak{B}$ that has at least two different extensions to a maximal ideal in $\mathfrak{A}$.

8.43. Prove that every ideal M in a relation algebra is the intersection of the system of maximal ideals that include M.

8.44. Prove Lemma 8.36 directly, without using Lemma 8.4.

8.45. Verify that conditions (i) and (ii) from Definition 8.7 are valid for the set $N = B \cap M$ in the proof of Lemma 8.40.

8.46. Complete the proof of the Second Isomorphism Theorem 8.43 by showing that the function φ preserves the operations of addition, complement, and converse.

8.47. An ideal M in a relation algebra $\mathfrak{A}$ is said to be *complete* if whenever X is a subset of M that has a supremum in $\mathfrak{A}$, then that supremum belongs to M. Prove that the kernel of a complete homomorphism is a complete ideal.

8.48. Prove that if M is a complete ideal (see Exercise 8.47), then the quotient mapping from $\mathfrak{A}$ to $\mathfrak{A}/M$ is a complete epimorphism with kernel M. Conclude that every complete ideal is the kernel of a complete epimorphism.

8.49. Prove that the quotient of a complete relation algebra by a complete ideal (see Exercise 8.47) is complete.

8.50. Prove that the annihilator of an ideal (see Exercise 8.20) is in fact a complete ideal.

8.51. Let M be an ideal in a relation algebra $\mathfrak{A}$, and B the Boolean algebra of ideal elements in $\mathfrak{A}$. Prove that the Boolean algebra of ideal elements in the quotient $\mathfrak{A}/M$ is isomorphic to the Boolean quotient $B/(B \cap M)$.

8.52. Prove Lemma 8.50.

8.53. The purpose of this exercise is to prove in detail that congruences can equivalently be replaced by filters instead of ideals.

(i) Prove that the cokernel of a congruence on a relation algebra is always a filter.
(ii) Prove that a congruence on a relation algebra is uniquely determined by its cokernel.
(iii) Prove that every filter in a relation algebra uniquely determines a congruence of which it is the cokernel.
(iv) Prove that the congruence classes of a congruence are just the cokernel cosets, that is to say, the sets of the form

$$r \Leftrightarrow N = \{r \Leftrightarrow s : s \in N\},$$

where N is the cokernel of the congruence.
(v) Describe the operations of the quotient of a relation algebra modulo a congruence Θ in terms of the cokernel cosets of the cokernel of Θ.
(vi) Prove that the quotient homomorphism from a relation algebra $\mathfrak{A}$ to a quotient $\mathfrak{A}/\Theta$ is just the mapping φ defined by $\varphi(r) = r \Leftrightarrow N$ for r in $\mathfrak{A}$, where N is the cokernel of Θ.

8.54. Prove directly that the intersection of a system of filters in a relation algebra is again a filter.

8.55. Formulate and prove the analogue of Lemma 8.11 for filters.

8.56. Prove directly (without using Theorem 8.12) that in a relation algebra, an element r belongs to the filter generated by a set X if and only if there is a finite subset Y of X such that $0 \mathbin{+\!\!,} (\prod Y) \mathbin{+\!\!,} 0 \leq r$. Conclude that every finitely generated filter is principal.

8.57. Prove that a filter N in a relation algebra $\mathfrak{A}$ is principal if and only if N has a smallest element. If such a smallest element r exists in N, prove that r must be an ideal element, and N must be the set of elements in $\mathfrak{A}$ that are above r.

8.58. Formulate and prove a version of Lemma 8.15 that applies to filters.

8.59. Formulate and prove a version of Lemma 8.16 that applies to filters.

8.60. A subset X of a relation algebra is said to have the *finite meet property* if, for every finite subset Y of X, the product

$$\prod\{0 \mathbin{+\!\!,} r \mathbin{+\!\!,} 0 : r \in Y\} = 0 \mathbin{+\!\!,} (\prod Y) \mathbin{+\!\!,} 0$$

is non-zero. Prove that a set X generates a proper filter if and only if X has the finite meet property.

8.61. Formulate and prove the analogue of Exercise 8.14 for filters.

8.62. Formulate and prove a version of Exercise 8.25 that applies to filters.

8.63. Prove that if M is an ideal in a relation algebra $\mathfrak{A}$, then the set

$$N = \{-r : r \in M\}$$

is a filter in $\mathfrak{A}$. This set is called the *dual filter* of M. Prove, conversely, that if N is a filter in $\mathfrak{A}$, then the set

$$M = \{-r : r \in N\}$$

is an ideal in $\mathfrak{A}$. This set is called the *dual ideal* of N.

8.64. Show that a set X generates an ideal M in a relation algebra if and only if the set $\{-r : r \in X\}$ generates the dual filter of M.

8.65. Define the notion of a complete filter in a relation algebra, and prove that an ideal is complete (see Exercise 8.47) if and only if its dual filter is complete.

8.66. The *cokernel* of a homomorphism is the set of elements in the domain that are mapped to 1. Prove that a homomorphism is one-to-one if and only if its cokernel is $\{1\}$.

8.67. Prove by a direct argument, without using Lemma 8.17, that if M and N are filters in a relation algebra $\mathfrak{A}$, then

$$M \vee N = \{r \cdot s : r \in M \text{ and } s \in N\}$$

and

$$M \wedge N = \{r + s : r \in M \text{ and } s \in N\}$$

in the lattice of filters of $\mathfrak{A}$.

8.68. Give a different proof of the result in Exercise 8.67, using the duality between ideals and filters together with Lemma 8.17.

8.69. Formulate and prove the analogue of Corollary 8.18 for filters.

8.70. Formulate the analogue of Theorem 8.22 for filters, and prove it using a direct argument, without appealing to Theorem 8.22 and the duality between ideals and filters.

8.71. Formulate the analogue of Theorem 8.23 for filters, and prove it using a direct argument, without appealing to Theorem 8.23 and the duality between ideals and filters.

8.72. Prove that the lattice of filters in a relation algebra is isomorphic to the lattice of Boolean filters in the corresponding Boolean algebra of ideal elements. Give a direct argument that does not appeal to the Lattice of Ideals Theorem and the duality between ideals and filters.

8.73. Verify that the dual of a principal ideal is a principal filter, and conversely. Conclude that the canonical isomorphism from the lattice of ideals to the lattice of filters in a relation algebra maps the sublattice of principal ideals onto the sublattice of principal filters.

8.74. Formulate a version of Lemma 8.29 that applies to filters. Give a direct proof that does not appeal to Lemma 8.29 and the duality between ideals and filters.

8.75. Formulate a version of Theorem 8.30 that applies to filters. Give a direct proof that does not make use of Theorem 8.30 and the duality between ideals and filters.

8.76. Formulate a version of the Maximal Ideal Theorem 8.31 that applies to filters. Give a direct proof that does not make use of Theorem 8.31 and the duality between ideals and filters.

8.77. Prove that every subset of a relation algebra with the finite meet property (see Exercise 8.60) is included in a maximal filter.

8.78. Let $\mathfrak{A}$ be an arbitrary Boolean algebra with normal operators. A subset M of $\mathfrak{A}$ is defined to be an ideal if it satisfies conditions (i)–(iii) of Definition 8.7 and the following condition in place of (iv).

(a) For every operator f of rank $n > 0$ in $\mathfrak{A}$, and every sequence of elements $r_0, \dots, r_{n-1}$ in $\mathfrak{A}$, if r_i is in M for some i, then $f(r_0, \dots, r_{n-1})$ is in M.

The goal of the following is to demonstrate that this notion of an ideal in a Boolean algebra with normal operators possesses all of the desired properties.

(i) Define the notion of a congruence on $\mathfrak{A}$, and show that the kernel of any congruence, that is to say, the congruence class of 0, is always an ideal in $\mathfrak{A}$.

(ii) Prove that if M is an ideal in $\mathfrak{A}$, and if Θ is the relation on the universe of $\mathfrak{A}$ that is defined by

$$r \equiv s \qquad \text{if and only if} \qquad r \ominus s \in M,$$

then Θ is a congruence on $\mathfrak{A}$, and M is the kernel of Θ. Show further that Θ is the only congruence on $\mathfrak{A}$ with kernel M.

(iii) Define the notion of the quotient of $\mathfrak{A}$ modulo an ideal M, and prove the analogues of Lemma 8.36, the Homomorphism Theorem, the Correspondence Theorem, and the three Isomorphism Theorems.

(iv) Prove that an ideal M in $\mathfrak{A}$ satisfies the following stronger version of condition (a): For every term definable, normal operation g of rank $n > 0$ on the universe of $\mathfrak{A}$, if $r_0, \dots, r_{n-1}$ are in $\mathfrak{A}$, and if r_i is in M for some i, then $g(r_0, \dots, r_{n-1})$ is in M.

8.79. The main results about ideals in relation algebras can be generalized to arbitrary Boolean algebras with normal operators $\mathfrak{A}$ in which there is a unary operation c that is term definable and that satisfies the following laws.

(a) $r \le c(r)$.
(b) $c(c(r)) \le c(r)$.
(c) $c(-c(r)) \le -c(r)$.
(d) $f(r_0, \dots, r_{n-1}) \le c(r_i)$ for every operator f of positive rank and every index $i = 0, \dots, n-1$.

The elements r in $\mathfrak{A}$ satisfying the equation $c(r) = r$ in $\mathfrak{A}$ are the analogues of ideal elements in relation algebras. Prove that the following laws hold in $\mathfrak{A}$.

(i) $c(r) = 0$ if and only if $r = 0$.
(ii) If $r \le s$, then $c(r) \le c(s)$.
(iii) $c(c(r)) = c(r)$.
(iv) $c(-c(r)) = -c(r)$.
(v) $c(r \cdot c(s)) = c(r) \cdot c(s)$.
(vi) $c(r + s) = c(r) + c(s)$.
(vii) $r \cdot c(s) = 0$ if and only if $s \cdot c(r) = 0$.

Conclude, in particular, that the elements r in $\mathfrak{A}$ satisfying the equation $c(r) = r$ form a Boolean subalgebra of the Boolean part of $\mathfrak{A}$.

8.80. Let $\mathfrak{A}$ be a Boolean algebra with normal operators in which there is a term definable unary operation c satisfying conditions (a)–(d) in Exercise 8.79. Prove the following assertions.

(i) An element r belongs to the ideal generated by a set X if and only if there is a finite subset Y of X such that $r \le c(\sum Y)$.
(ii) Every principal ideal M has a largest element r, and $c(r) = r$. The elements of M are just the elements in $\mathfrak{A}$ that are below r.
(iii) Every finitely generated ideal in $\mathfrak{A}$ is principal.
(iv) For an arbitrary ideal M in $\mathfrak{A}$, and an arbitrary element r_0 in $\mathfrak{A}$, the ideal generated by the set $M \cup \{r_0\}$ is

$$N = \{r + s : r \le c(r_0) \text{ and } s \in M\}.$$

(v) An ideal M is improper just in case, for some element r in $\mathfrak{A}$, both r and $-c(r)$ are in M.
(vi) An ideal M is maximal if and only if, for every element r in $\mathfrak{A}$, exactly one of r and $-c(r)$ is in M.

(vii) For every principal ideal L in $\mathfrak{A}$, and every ideal M that is properly included in L, there is an ideal that is maximal in L and includes M.

(viii) For every proper ideal M in $\mathfrak{A}$, and every element r that does not belong to M, there is a maximal ideal that includes M and does not contain r.

8.81. Let $\mathfrak{A}$ be a Boolean algebra with normal operators in which there is a term definable unary operation c satisfying conditions (a)–(d) in Exercise 8.79. Formulate and prove versions of Lemmas 8.40–8.42.

8.82. Let $\mathfrak{A}$ be a Boolean algebra with normal operators in which there is a term definable unary operation c satisfying conditions (a)–(d) in Exercise 8.79. Formulate and prove a version of the Second Isomorphism Theorem 8.43.

8.83. Let $\mathfrak{A}$ be a Boolean algebra with normal operators in which there is a term definable unary operation c satisfying conditions (a)–(d) in Exercise 8.79. Formulate and prove a version of the Homomorphism Extension Theorem 8.46.

Chapter 9
Simple algebras

Every homomorphic image of a relation algebra $\mathfrak{A}$ is isomorphic to a quotient of $\mathfrak{A}$ modulo some ideal, by the First Isomorphism Theorem 8.39. Larger ideals lead to structurally simpler homomorphic images than smaller ideals, because larger ideals "glue" more elements together than smaller ones. More precisely, whenever an ideal M (in $\mathfrak{A}$) is included in an ideal N, then the quotient $\mathfrak{A}/N$ is a homomorphic image of the quotient $\mathfrak{A}/M$, by the Third Isomorphism Theorem 8.48. This leads to a rough classification of the homomorphic images of $\mathfrak{A}$ according to the location, in the lattice of ideals, of the ideal corresponding to each homomorphic image (via the First Isomorphism Theorem): structurally simpler homomorphic images of $\mathfrak{A}$ correspond to ideals that are toward the top of the lattice, while structurally more complicated homomorphic images correspond to ideals that are toward the bottom. From this perspective, the simplest non-degenerate homomorphic images of $\mathfrak{A}$ correspond to proper ideals that are just below the top of the lattice, that is to say, they correspond to the maximal ideals of $\mathfrak{A}$.

These simplest non-degenerate homomorphic images are called simple algebras, and they play a fundamental role in the theory of relation algebras. They form the building blocks from which all relation algebras can be constructed. For example, as we shall see in Corollary 11.45 and Theorem 12.10 respectively, every finite relation algebra is isomorphic to a direct product of simple homomorphic images, and every relation algebra is isomorphic to a subalgebra of a direct product of simple homomorphic images.

The purpose of this chapter is to study the class of simple relation algebras. Within this class, a special subclass of algebras can be

S. Givant, *Introduction to Relation Algebras*,
DOI 10.1007/978-3-319-65235-1_9

distinguished by a certain integrality condition, and many interesting examples of relation algebras turn out to satisfy this integrality condition.

9.1 Simple relation algebras

A relation algebra $\mathfrak{A}$ is called *simple* if it is not degenerate and if every homomorphism on $\mathfrak{A}$ is either a monomorphism or else has the degenerate (one-element) relation algebra as its range. In view of the First Isomorphism Theorem, this definition is equivalent to saying that $\mathfrak{A}$ is simple if and only if it has exactly two ideals: the trivial ideal $\{0\}$ and the improper ideal A (and these two ideals do not coincide). The lattice of ideals in $\mathfrak{A}$ is isomorphic to the lattice of Boolean ideals in the Boolean algebra of ideal elements in $\mathfrak{A}$, by the Lattice of Ideals Theorem 8.26, so the simplicity of $\mathfrak{A}$ is equivalent to the assertion that the Boolean algebra of ideal elements in $\mathfrak{A}$ has exactly two ideals, or, put another way, the Boolean algebra of ideal elements in $\mathfrak{A}$ is simple (as a Boolean algebra). The set of elements below any given element r in a Boolean algebra is easily seen to be a Boolean ideal (it is the principal Boolean ideal generated by r), so a Boolean algebra is simple if and only if it consists of exactly two elements, 0 and 1. This proves the following lemma.

Lemma 9.1. *A relation algebra is simple if and only if it has exactly two* (*distinct*) *ideal elements*, 0 *and* 1.

In other words, a relation algebra is simple if and only if the unit is an ideal element atom.

One consequence of the lemma is the surprising fact that the notion of simplicity for relation algebras is characterizable by a universal sentence in the (first-order) language of relation algebras. In fact, there are various interesting universal sentences that can serve this purpose. We give some of them in the following *Simplicity Theorem*. It should be pointed out that the notion of simplicity for general classes of algebras is rarely characterizable by a set of first-order sentences.

Theorem 9.2. *The following conditions on a relation algebra* $\mathfrak{A}$ *are equivalent*.

(i) $\mathfrak{A}$ *is simple*.

(ii) $0 \neq 1$, *and for all* r *in* $\mathfrak{A}$, *if* $r \neq 0$, *then* $1 ; r ; 1 = 1$.
(iii) $0 \neq 1$, *and for all* r *in* $\mathfrak{A}$, *either* $r ; 1 = 1$ *or* $1 ; -r = 1$.
(iv) $0 \neq 1$, *and for all* r, s *in* $\mathfrak{A}$, *if* $r ; 1 ; s = 0$, *then* $r = 0$ *or* $s = 0$.

Proof. We shall show that (ii) is equivalent with each of the other conditions. Condition (ii) says in effect that $\mathfrak{A}$ has precisely two ideal elements, 0 and 1, so the equivalence of (i) and (ii) follows from Lemma 9.1.

Turn now to the equivalence of (ii) and (iii), and consider first the implication from (ii) to (iii). Let r be any element in $\mathfrak{A}$. If $r ; 1 = 1$, then (iii) holds trivially. If $r ; 1 \neq 1$, then $-(r ; 1) \neq 0$, by Boolean algebra, so

$$1 ; -(r ; 1) ; 1 = 1, \tag{1}$$

by condition (ii). Lemma 4.4(iii) (with r and s replaced by 1 and r respectively) says that

$$-(r ; 1) ; 1^{\smile} + -r = -r,$$

or equivalently, using also Lemma 4.1(vi),

$$-(r ; 1) ; 1 \leq -r.$$

Form the relative product of both sides of this inequality with 1 on the left, and use the monotony law for relative multiplication, to obtain

$$1 ; -(r ; 1) ; 1 \leq 1 ; -r. \tag{2}$$

Combine (1) and (2) to arrive at $1 ; -r = 1$. Thus, (iii) holds

To establish the reverse implication, assume that (iii) holds, and replace r by $1 ; r$ in (iii) to obtain

$$1 ; r ; 1 = 1 \qquad \text{or} \qquad 1 ; -(r ; 1) = 1. \tag{3}$$

Axiom (R10) (with r and s replaced by 1 and r respectively) says that

$$1^{\smile} ; -(1 ; r) + -r = -r,$$

or equivalently, using also Lemma 4.1(vi),

$$1 ; -(1 ; r) \leq -r.$$

Consequently, the second equation in (3) implies that $-r = 1$, or what amounts to the same thing, that $r = 0$. Thus, we have either $r = 0$ or else $1 ; r ; 1 = 1$, by (3), and this is just what (ii) asserts.

It remains to establish the equivalence of (ii) and (iv). Assume first that (ii) holds. If $r\,;1\,;s = 0$ and $r \neq 0$, then $1\,;r\,;1 = 1$, by (ii), and therefore

$$0 = 1\,;0 = 1\,;(r\,;1\,;s) = (1\,;r\,;1)\,;s = 1\,;s \geq s,$$

by Corollary 4.17, the assumption about $r\,;1\,;s$, the associative law for relative multiplication, the assumption about r, and the first dual of Lemma 4.5(iii). Consequently, $s = 0$, so we obtain (iv).

Assume next that (iv) holds, and consider any element r in $\mathfrak{A}$. Axiom (R10) (with r and s replaced by $1\,;r^{\smile}$ and 1 respectively) implies that

$$(1\,;r^{\smile})^{\smile}\,;-(1\,;r^{\smile}\,;1) + 0 = 0. \tag{4}$$

We have

$$(1\,;r^{\smile})^{\smile} = r\,;1 \qquad \text{and} \qquad 1\,;r^{\smile}\,;1 = 1\,;r\,;1, \tag{5}$$

by the involution laws, Lemma 4.1(vi), and Corollary 5.42, so (4) and (5) may be combined to conclude (with the help of Boolean algebra) that

$$r\,;1\,;-(1\,;r\,;1) = 0. \tag{8}$$

If $r \neq 0$, then $-(1\,;r\,;1) = 0$, by (8) and (iv) (with $-(1\,;r\,;1)$ in place of s), and therefore $1\,;r\,;1 = 1$, by Boolean algebra. Thus, (ii) holds. □

It may be noted in passing that the second part of condition (iv) is equivalent to the condition that a rectangle can equal zero only if one of its sides is zero.

A consequence of the preceding theorem is the important observation that the property of simplicity is inherited by subalgebras.

Corollary 9.3. *Every subalgebra of a simple relation algebra is simple.*

Proof. A relation algebra $\mathfrak{A}$ is simple if and only if one of the universal sentences in the preceding theorem—for instance, (ii)— is true in $\mathfrak{A}$. Universal sentences are preserved under the passage to subalgebras, by Corollary 6.4, so (ii) holds in $\mathfrak{A}$ if and only if it holds in all subalgebras of $\mathfrak{A}$. Thus, $\mathfrak{A}$ is simple if and only if all subalgebras of $\mathfrak{A}$ are simple. □

The preceding lemma, theorem, and corollary greatly facilitate the task of showing that a given relation algebra is, or is not, simple. For example, the full relation algebra $\mathfrak{Re}(U)$ on a non-empty set U is simple, because condition (ii) in Theorem 9.2 is easily seen to hold in $\mathfrak{Re}(U)$. In more detail, the set U is assumed to be non-empty, so the unit $U \times U$ is certainly different from the zero element $\varnothing$. Consider now any non-empty relation R in $\mathfrak{Re}(U)$, and suppose that (α, β) is a pair of elements in R. For any elements γ and δ in U, the pairs (γ, α) and (β, δ) belong to the unit $U \times U$, so the pair (γ, δ) belongs to the composition

$$(U \times U) \mid R \mid (U \times U),$$

by the definition of relational composition. Consequently, this composition coincides with the unit $U \times U$, so condition (ii) holds in $\mathfrak{Re}(U)$. It follows from Theorem 9.2 and Corollary 9.3 that $\mathfrak{Re}(U)$ and each of its subalgebras is simple, that is to say, every algebra of relations on a non-empty set is simple. In particular, the minimal set relation algebras $\mathfrak{M}_1$, $\mathfrak{M}_2$, and $\mathfrak{M}_3$ are simple (see Section 3.1).

On the other hand, the full set relation algebra $\mathfrak{Re}(E)$ on an equivalence relation E with at least two equivalence classes is never simple. Indeed, if V is any equivalence class of E, then the relation $V \times V$ is an ideal element in $\mathfrak{Re}(E)$ that is different from both the zero element $\varnothing$ and the unit E, so $\mathfrak{Re}(E)$ has more than two ideal elements and is therefore not simple, by Lemma 9.1. Warning: this argument shows that $\mathfrak{Re}(E)$ is not simple, but it is perfectly possible for some subalgebras of $\mathfrak{Re}(E)$ to be simple.

For yet another example, observe that every element in a Boolean relation algebra $\mathfrak{A}$ is an ideal element, since relative multiplication coincides with Boolean multiplication in $\mathfrak{A}$. Indeed, if r is any element in $\mathfrak{A}$, then

$$1 ; r ; 1 = 1 \cdot r \cdot 1 = r,$$

so r is an ideal element in $\mathfrak{A}$. Consequently, a Boolean relation algebra is simple if and only if it has exactly two elements, by Lemma 9.1. Put another way, a Boolean relation algebra is simple if and only if it is isomorphic to $\mathfrak{M}_1$.

There is an interesting kind of converse to Corollary 9.3. A first-order universal sentence with a single variable is valid in an algebra if and only if it is valid in every 1-*generated subalgebra*, that is to say, in every subalgebra generated by a single element. Since simplicity can

be expressed by a universal sentence with a single variable, we obtain the following conclusion.

Corollary 9.4. *If every* 1*-generated subalgebra of a relation algebra* $\mathfrak{A}$ *is simple*, *then* $\mathfrak{A}$ *is simple.*

Another consequence of Theorem 9.2 is that every quantifier-free formula in the (first-order) language of relation algebras is equivalent to an equation in all simple relation algebras.

Theorem 9.5. *For every quantifier-free formula* Γ *in the language of relation algebras*, *there is a term* γ *with the same free variables as* Γ *such that* Γ *and the equation* $\gamma = 0$ *are equivalent in all simple relation algebras.*

Proof. The proof proceeds by induction on the definition of quantifier-free formulas in the language of relation algebras. If Γ is an equation, say $\sigma = \tau$, then take γ to be the term $\sigma \ominus \tau$, that is to say, the term

$$\sigma \cdot -\tau + -\sigma \cdot t.$$

The definition of $\ominus$ implies that a sequence of elements in a relation algebra satisfies the equation $\sigma = \tau$ if and only if it satisfies the equation $\sigma \ominus \tau = 0$, so Γ is equivalent to the equation $\gamma = 0$ in all simple relation algebras (and in fact in all relation algebras).

Next, suppose Γ has the form $\neg\Delta$ for some quantifier-free formula Δ, and assume as the induction hypothesis that Δ is equivalent to an equation $\delta = 0$ in all simple relation algebras. The negation $\neg\Delta$ is then equivalent to the inequality $\delta \neq 0$ in all simple relation algebras. For every element r in a simple relation algebra,

$$r \neq 0 \qquad \text{if and only if} \qquad 1 \mathbin{;} r \mathbin{;} 1 = 1,$$

by Theorem 9.2(ii) and Corollary 4.17. Consequently, $\neg\Delta$ is equivalent to the equation $1 \mathbin{;} \delta \mathbin{;} 1 = 1$ in all simple relation algebras. Take γ to be the term $-(1 \mathbin{;} \delta \mathbin{;} 1)$, or the equivalent term $0 \mathbin{\underset{,}{+}} (-\delta) \mathbin{\underset{,}{+}} 0$, to conclude that Γ is equivalent to the equation $\gamma = 0$ in all simple relation algebras.

Finally, suppose Γ has the form $\Delta \wedge \Xi$ for some quantifier-free formulas Δ and Ξ, and assume as the induction hypothesis that Δ and Ξ are respectively equivalent to equations $\delta = 0$ and $\xi = 0$ in all simple relation algebras. The conjunction $\Delta \wedge \Xi$ is then equivalent to the

conjunction of the equations $\delta = 0$ and $\xi = 0$ in all simple relation algebras. For every pair of elements r and s in a relation algebra,

$$r = 0 \text{ and } s = 0 \qquad \text{if and only if} \qquad r + s = 0,$$

by Boolean algebra. Take γ to be the term $\delta + \xi$ to conclude that Γ is equivalent to the equation $\gamma = 0$ in all simple relation algebras. □

The preceding theorem is sometimes called the *Schröder-Tarski Translation Theorem* because it gives an effective method for translating every quantifier-free formula into an equivalent equation (with respect to the class of simple relation algebras). In connection with this result, it may be remarked that—as we shall see in Theorem 12.11—an equation is true in all relation algebras if and only if it is true in all simple relation algebras.

Turn now to the question of when the quotient of a relation algebra $\mathfrak{A}$ modulo an ideal M is simple. To say that such a quotient is simple is to say that it has exactly two ideals. The lattice of ideals in the quotient is isomorphic to the sublattice of ideals in $\mathfrak{A}$ that include M, by the Correspondence Theorem 8.47. Consequently, the quotient algebra $\mathfrak{A}/M$ is simple if and only if there are exactly two ideals in $\mathfrak{A}$ that include M, namely M and A. In other words, the quotient algebra is simple if and only if M is a maximal ideal.

Lemma 9.6. *A quotient relation algebra $\mathfrak{A}/M$ is simple if and only if the ideal M is maximal in $\mathfrak{A}$.*

Notice that the condition in the lemma precludes the possibility that the algebra $\mathfrak{A}$ and its quotient $\mathfrak{A}/M$ are degenerate. Indeed, the degenerate algebra has only one ideal, namely the improper ideal, and the improper ideal cannot be maximal, by the definition of a maximal ideal.

9.2 Integral relation algebras

We turn now to a special class of relation algebras that turn out to be simple. A relation algebra is called *integral* if it is not degenerate, and if it has no zero divisors, that is to say, for all elements r and s,

$$r \,;\, s = 0 \qquad \text{implies} \qquad r = 0 \quad \text{or} \quad s = 0.$$

Integral relation algebras are characterized by a number of rather surprising properties, each of which is expressible as a universal sentence in the language of relation algebras. We gather some of these together in the following *Integrality Theorem*.

Theorem 9.7. *The following conditions on a relation algebra* $\mathfrak{A}$ *are equivalent.*

(i) $\mathfrak{A}$ *is integral.*
(ii) $0 \neq 1$ *and* $r\,;1 = 1$ *for every non-zero element* r *in* $\mathfrak{A}$*.*
(iii) $0 \neq 1$ *and* $1\,;r = 1$ *for every non-zero element* r *in* $\mathfrak{A}$*.*
(iv) $0 \neq 1$ *and all non-zero elements have domain* 1'.
(v) $0 \neq 1$ *and all non-zero elements have range* 1'.
(vi) $0 \neq 1$ *and all non-zero functions are atoms.*
(vii) 1' *is an atom.*

Proof. The equivalence of (ii) and (iii) is a consequence of the first duality principle, as is the equivalence of (iv) and (v). For example, to establish the implication from (iv) to (v), assume that

$$(r\,;1)\cdot 1' = 1'$$

for all non-zero elements r in $\mathfrak{A}$. Since r is non-zero if and only if $r^{\smile}$ is non-zero, by Lemma 4.1(vi), we may replace r by $r^{\smile}$ in the preceding equation, form the converse of both sides of the resulting equation, and apply the involution laws and the laws in Lemmas 4.1 and 4.3 to conclude that

$$(1\,;r)\cdot 1' = 1'$$

for all non-zero elements r in $\mathfrak{A}$. The reverse implication, from (v) to (iv), is established in a completely analogous way.

In view of the preceding remarks, it suffices to prove the implications from (i) to (ii), from (ii) to (iv), from (iv) to (vi), from (vi) to (vii), and from (vii) to (i). For the implication from (i) to (ii), recall that

$$r^{\smile}\,;-(r\,;1) = 0$$

for every element r in $\mathfrak{A}$, by Lemma 4.11. If $\mathfrak{A}$ is integral, then of course $0 \neq 1$, and the preceding equation implies that

$$r^{\smile} = 0 \qquad \text{or} \qquad -(r\,;1) = 0.$$

In the first case, we have $r = 0$, by Lemma 4.1(vi), and in the second case, $r\,;1 = 1$, by Boolean algebra, so (ii) holds.

If (ii) holds, then for any non-zero element r in $\mathfrak{A}$, we have

$$\text{domain } r = (r\,;1)\cdot 1\text{'} = 1\cdot 1\text{'} = 1\text{'},$$

by the definition of the domain of r, (ii), and Boolean algebra, so (iv) holds.

To establish the implication from (iv) to (vi), assume that r is a non-zero function (see Section 5.8), and consider any non-zero element s below r, with the goal of showing that $s = r$. Observe that s is a function, by Lemma 5.66(ii), so if (iv) holds, then

$$1\text{'} = (s\,;1)\cdot 1\text{'} \le s\,;s^{\smile}\,;1\text{'} = s\,;s^{\smile}, \tag{1}$$

by the assumption in (iv) applied to s, the definition of the domain of an element, Corollary 4.21 (with s, 1, and 1' in place of r, s, and t respectively), and the identity law for relative multiplication. Since

$$s^{\smile} \le r^{\smile} \qquad \text{and} \qquad r^{\smile}\,;r \le 1\text{'}, \tag{2}$$

by Lemma 4.1(i) and the assumptions on r and s, we obtain

$$r = 1\text{'}\,;r \le s\,;s^{\smile}\,;r \le s\,;r^{\smile}\,;r \le s\,;1\text{'} = s,$$

by the identity and monotony laws for relative multiplication, and (1) and (2). Conclusion: every non-zero element below r must coincide with r, so r is an atom. Thus, (vi) holds.

For the implication from (vi) to (vii), observe that $1\text{'} \ne 0$, because $\mathfrak{A}$ is assumed to be non-degenerate. In more detail, $1\text{'} = 0$ implies that

$$1 = 1\,;1\text{'} = 1\,;0 = 0,$$

by the identity law for relative multiplication and Corollary 4.17. Consequently, 1' is a non-zero function, by Lemma 5.66(i). The assumption in (vi) therefore implies that 1' is an atom.

Turn finally to the implication from (vii) to (i). Certainly, $\mathfrak{A}$ is non-degenerate, since 1' is an atom (degenerate relation algebras have no atoms). Let r and s be elements in $\mathfrak{A}$ such that $r\,;s = 0$. The domain of every element is, by definition, below 1', so the assumption that (vii) holds implies that the domain of s is either 0 or 1'. In the first case, we have $(s\,;1)\cdot 1\text{'} = 0$, by the definition of the domain of s, and

therefore $(1' ; 1^{\smile}) \cdot s = 0$, by the De Morgan-Tarski laws (Lemma 4.8). This last equation implies that $s = 0$, by Lemma 4.1(vi), the identity law for relative multiplication, and Boolean algebra. In the second case,

$$(s ; 1) \cdot 1' = 1', \tag{3}$$

and therefore

$$r = r ; 1' = r ; [(s ; 1) \cdot 1'] \leq r ; (s ; 1) = (r ; s) ; 1 = 0 ; 1 = 0,$$

by the identity law for relative multiplication, (3), the monotony and associative laws for relative multiplication, the assumption on $r ; s$, and the first dual of Corollary 4.17. Thus, $\mathfrak{A}$ is integral. □

The sentences characterizing integral relation algebras in the previous lemma are universal in form, and most of them involve just one variable. Consequently, the same types of arguments that are used to prove Corollaries 9.3 and 9.4 can be used to establish the analogues of these corollaries for integral relation algebras.

Corollary 9.8. *Every subalgebra of an integral relation algebra is integral.*

Corollary 9.9. *If every* 1*-generated subalgebra of a relation algebra* $\mathfrak{A}$ *is integral, then* $\mathfrak{A}$ *is integral.*

There is a close connection between the definition of an integral relation algebra and condition (iv) in Theorem 9.2. In fact, the latter might be viewed as a kind of weak integrality condition. It is therefore perhaps not surprising that integral relation algebras turn out to be simple.

Corollary 9.10. *Every integral relation algebra is simple.*

Proof. For any non-zero element r in an integral relation algebra $\mathfrak{A}$,

$$1 ; r ; 1 = 1 ; 1 = 1,$$

by Theorem 9.7(ii) and Lemma 4.5(iv). Consequently, $\mathfrak{A}$ is simple, by Theorem 9.2. □

The Integrality Theorem greatly facilitates the task of determining whether a given relation algebra is, or is not, integral. For example,

the identity element in the complex algebra of any group G is the singleton of the group identity element in G, so it is certainly an atom in $\mathfrak{Cm}(G)$. Thus, every group complex algebra is integral and therefore simple. Similarly, the identity element in the complex algebra of any geometry P is the singleton of the new element ι that is adjoined to P to form the complex algebra, so it is clearly an atom in $\mathfrak{Cm}(P)$. Consequently, every geometric complex algebra is integral and simple. The identity element is also an atom in the minimal relation algebras $\mathfrak{M}_1$, $\mathfrak{M}_2$, and $\mathfrak{M}_3$, so these algebras are integral as well.

By way of contrast with the preceding examples, observe that the identity element is never an atom in the full set relation algebra on a set U of cardinality at least two, so $\mathfrak{Re}(U)$ is never integral when U has more than one element. It follows that the converse of Corollary 9.10 is false: a simple relation algebra need not be integral. The same example shows that a subalgebra of a non-integral simple relation algebra may in fact be integral, since the minimal subalgebra of $\mathfrak{Re}(U)$ is integral whenever U is non-empty.

Another interesting property of integral relation algebras is that the non-zero bijections in the algebra (see Section 5.8) form a group.

Lemma 9.11. *In an integral relation algebra, the set of non-zero bijections is a group of atoms under the operations of relative multiplication and converse, with* 1' *as the identity element. If r is an atom and s a non-zero bijection, then the products $s\,;r$ and $r\,;s$ are atoms, and they are bijections just in case r is a bijection.*

Proof. Non-zero bijections are permutations, and also atoms, in an integral relation algebra, by Theorem 9.7(iv)–(vi), so the set of non-zero bijections coincides with the set of permutations and is a subset of the set of atoms. In particular, this set is a group of atoms under the operations of relative multiplication and converse, with 1' as the identity element, by Lemma 5.87.

To prove the second assertion of the lemma, consider an atom r and a non-zero bijection s. We have

$$1' = \text{domain } r = \text{range } r = \text{domain } s = \text{range } s,$$

by parts (iv) and (v) of Theorem 9.7, so $r\,;s$ and $s\,;r$ are atoms, by Lemma 5.86(ii) and its first dual. If r is a bijection, then so is $r\,;s$, by the first assertion of the present lemma. Conversely, if $r\,;s$ is a bijection, then so is $r\,;s\,;s^{\smile}$, by the first assertion of the lemma; since

$$r\,;s\,;s^{\smile} = r\,;1' = r,$$

it may be concluded that r is a bijection. $\square$

9.3 Directly and subdirectly indecomposable algebras

There are two further algebraic notions that are closely related to, but usually weaker than, the notion of simplicity. An algebra is called *directly indecomposable* if it is non-degenerate and cannot be written as—that is to say, it is not isomorphic to—the direct product of two non-degenerate algebras. As we shall see in Corollary 11.12, a relation algebra turns out to be directly indecomposable just in case it is non-degenerate and for any two ideal elements r and s in the algebra,

$$r\cdot s = 0 \quad \text{and} \quad r+s=1 \qquad \text{implies} \qquad r=0 \quad \text{or} \quad s=0.$$

This condition says that there is no non-trivial partition of the unit by ideal elements. On the set of ideal elements, the operations of relative addition and multiplication coincide with their Boolean counterparts, by Lemma 5.41, so the preceding implication can be rewritten as

$$r\,;s = 0 \quad \text{and} \quad r \mathbin{+\!\!\!\!,\,} s=1 \qquad \text{implies} \qquad r=0 \quad \text{or} \quad s=0.$$

Notice the resemblance of this implication to the condition of integrality discussed in the preceding section.

An algebra is called *subdirectly irreducible* if it is non-degenerate and cannot be written as a subdirect product of two or more non-degenerate algebras. As we shall see in Lemma 12.9(iii), a relation algebra turns out to be subdirectly irreducible just in case it is non-degenerate and for any system $(r_i : i \in I)$ of ideal elements in the algebra, if the infimum of the system is zero, then at least one of the elements in the system is zero, that is to say,

$$\textstyle\prod_i r_i = 0 \qquad \text{implies} \qquad r_i = 0$$

for some i.

Quite surprisingly, in relation algebras the two notions just defined coincide with the notion of simplicity.

Theorem 9.12. *In a relation algebra $\mathfrak{A}$, the following conditions are equivalent.*

(i) $\mathfrak{A}$ *is simple.*
(ii) $\mathfrak{A}$ *is subdirectly irreducible.*
(iii) $\mathfrak{A}$ *is directly indecomposable.*

Proof. A simple relation algebra $\mathfrak{A}$ is non-degenerate and has just two ideal elements, 0 and 1, by Lemma 9.1. Consequently, if the product of a system of ideal elements in $\mathfrak{A}$ is 0, then at least one of the ideal elements must obviously be 0. Thus, $\mathfrak{A}$ is subdirectly irreducible, by the remarks preceding the theorem, so condition (i) implies condition (ii).

A subdirectly irreducible relation algebra $\mathfrak{A}$ is non-degenerate, and the product of two non-zero ideal elements is always non-zero, by the remarks preceding the theorem. Consequently, there can be no non-trivial partition of the unit, so $\mathfrak{A}$ is directly indecomposable. Thus, condition (ii) implies condition (iii).

The implication from (iii) to (i) is established via an argument by contraposition. If $\mathfrak{A}$ is non-degenerate but not simple, then there must be an ideal element r that is different from 0 and 1, by Lemma 9.1. The complement $-r$ is also an ideal element, by Lemma 5.39(iv), and the two ideal elements r and $-r$ form a non-trivial partition of the unit. Consequently, $\mathfrak{A}$ cannot be directly indecomposable, by the remarks preceding the theorem. □

It is now easy to see that subdirect irreducibility can be characterized by a weaker condition than the one mentioned before the theorem.

Corollary 9.13. *A relation algebra is subdirectly irreducible if and only if it is non-degenerate and the product of two non-zero ideal elements is always non-zero.*

Proof. By Theorem 9.12 it suffices to prove the corollary with “simple” in place of “subdirectly irreducible”. If a relation algebra $\mathfrak{A}$ is simple, then the condition in the corollary obviously holds, by Lemma 9.1. On the other hand, if the condition in the corollary holds, then $\mathfrak{A}$ cannot have an ideal element r different from 0 or 1, because the elements r and $s = -r$ would satisfy the hypothesis, but not the conclusion, of the condition. Consequently, $\mathfrak{A}$ must be simple, by Lemma 9.1. □

For a non-degenerate relation algebra, the condition in the corollary is equivalent to the requirement that for any two ideal elements r and s,

$$r \mathbin{;} s = 0 \qquad \text{implies} \qquad r = 0 \quad \text{or} \quad s = 0,$$

by Lemma 5.41(ii). Thus, a non-degenerate relation algebra is subdirectly irreducible just in case the condition defining integrality applies to the set of ideal elements.

9.4 Historical remarks

Peirce and Schröder always worked in the context of the full relation algebra on some set, so implicitly they always dealt with simple relation algebras. The explicit study of simple relation algebras as a special subclass of the class of all relation algebras dates back to McKinsey and Tarski. In particular, Lemma 9.1 and the characterizations of simplicity in terms of conditions (ii) and (iv) in the Simplicity Theorem are due to them, and are mentioned in [55] (see also [53]). The characterization of simplicity in terms of condition (iii) in the theorem is taken from Tarski [105] (see also [112]). Corollary 9.3, stating that subalgebras of simple relation algebras are simple, is given in [55], while Corollary 9.4 is due to Tarski [112].

The equivalences underlying the proof of the Schröder-Tarski Translation Theorem (in the implicit context of full relation algebras on sets) date back to Schröder [98], pp. 150–153. The derivations of these equivalences in the context of simple relation algebras and the formulation of Theorem 9.5 are due to Tarski. The theorem is explicitly mentioned in [110].

Integral relation algebras are mentioned for the first time by Jónsson and Tarski in the abstract [53]. The characterizations of integrality in terms of conditions (ii), (vi), and (vii) are due to Jónsson and Tarski [55]. The remaining characterizations in the theorem (due to Givant) were obtained by analyzing the proofs involved in the Jónsson-Tarski characterizations. Corollaries 9.8 and Corollary 9.10 are also due to Jónsson and Tarski [55], while Corollary 9.9 and Lemma 9.11 are due to Givant.

Small integral relation algebras—those that are finite and have at most six atoms—have been extensively studied by a number of people including (in roughly chronological order) Roger Lyndon [68], Ralph McKenzie [82], [83], Ulf Wostner [121], Roger Maddux [71], [78], Stephen Comer [24], [25], Peter Jipsen [46], Peter Jipsen and Erzsébet Lukács [48], and Hajnal Andréka and Roger Maddux [6]. Some of this

work has been done with the help of a computer (see, for example, Chapter 8 in [78]).

The equivalence of conditions (i) and (iii) in Theorem 9.12 is due Jónsson and Tarski [55]. The equivalence of conditions (i) and (ii) in the theorem is not given in [55], but Jónsson and Tarski may have been aware of it. The equivalence is explicitly stated and proved by Tarski in [112]. The result in Exercise 9.2 is proved in Tarski [111].

The study of (ternary) discriminator functions in arbitrary algebras (and not just in Boolean algebras with normal operators) dates back to the work of Alden Pixley, who proved in [89] that every non-degenerate algebra with a discriminator function is simple (see Exercise 9.8). Discriminator varieties were studied by Heinrich Werner, who proved in [116], [117], [118] (see also [119]) that in such a variety the notions of simplicity, subdirect irreducibility, and direct indecomposability coincide, and also that every open formula is equivalent to an equation in all simple algebras in the variety (see Exercise 9.18). The result in Exercise 9.16 is from [5] and improves an earlier result of Jipsen [47].

Exercises

9.1. Consider the following condition on a relation algebra: for all elements r, we have $r\,;1 \neq 1$ if and only if $1\,;-r = 1$. Is it true that a relation algebra $\mathfrak{A}$ is simple if and only if this condition holds in $\mathfrak{A}$?

9.2. Prove that a simple relation algebra is minimal if and only if the equation

$$r\,;1\,;-r\,;1\,;(r\cdot 1\text{'} + -r\cdot 0\text{'})\,;1\,;(r\cdot 0\text{'} + -r\cdot 1\text{'}) = 0$$

is true in the algebra.

9.3. Suppose two elements r and s in a relation algebra $\mathfrak{A}$ generate distinct ideal elements. Prove that there is a homomorphism φ from $\mathfrak{A}$ onto a simple relation algebra that distinguishes r and s in the sense that $\varphi(r) \neq \varphi(s)$.

9.4. Prove the following addition to the Homomorphism Extension Theorem 8.46. If $\mathfrak{B}$ is a subalgebra of a relation algebra $\mathfrak{A}$, then every homomorphism from $\mathfrak{B}$ onto a simple relation algebra $\mathfrak{C}$ can be extended to a homomorphism from $\mathfrak{A}$ onto a simple relation algebra $\mathfrak{D}$ that includes $\mathfrak{C}$ as a subalgebra.

9.5. Call two homomorphisms on a relation algebra *dissimilar* if they have different kernels. Suppose $\mathfrak{B}$ is a subalgebra of a relation algebra $\mathfrak{A}$ that does not contain all of the ideal elements of $\mathfrak{A}$. Prove that there is a homomorphism from $\mathfrak{B}$ onto a simple relation algebra that can be extended to two dissimilar homomorphisms from $\mathfrak{A}$ onto simple relation algebras.

9.6. Suppose $\mathfrak{A}$ is the formula relation algebra of an elementary language $\mathcal{L}^*$ of relations modulo a set of formulas $\mathcal{S}$ in $\mathcal{L}^*$ (see Section 3.3). If $\mathcal{S}$ is complete in the sense that every sentence in $\mathcal{L}^*$ or its negation is derivable from $\mathcal{S}$, and consistent in the sense that not every sentence in $\mathcal{L}^*$ is derivable from $\mathcal{S}$, prove that $\mathfrak{A}$ must be simple.

9.7. Which of the algebras in Exercises 3.36–3.39 are simple? Which of them are integral?

9.8. Which of the algebras in Exercises 3.40–3.41 are simple? Which of them are integral?

9.9. Prove directly (without using the Simplicity Theorem 9.2) that the full relation algebra $\mathfrak{Re}(U)$ is simple for every non-empty set U.

9.10. Suppose the formulas $\varDelta$ and $\varXi$ in the proof of Theorem 9.5 are respectively equivalent to the equations $\delta = 0$ and $\xi = 0$ in all simple relation algebras. If $\varGamma$ is the formula $\varDelta \vee \varXi$, how should the term γ be defined so that $\varGamma$ and $\gamma = 0$ are equivalent in all simple relation algebras? What if $\varGamma$ is the formula $\varDelta \rightarrow \varXi$?

9.11. The Schröder-Tarski Translation Theorem has the following dual version that is also useful: for every quantifier-free formula $\varGamma$ in the language of relation algebras, there is a term γ with the same free variables as $\varGamma$ such that $\varGamma$ and the equation $\gamma = 1$ are equivalent in all simple relation algebras. Prove this dual version directly (without using Theorem 9.5).

9.12. Prove that the complex algebra of a modular lattice with zero (see Section 3.7) is integral and therefore simple.

9.13. Prove directly (without using the Integrality Theorem 9.7) that the complex algebra of a group is integral and therefore simple.

9.14. Prove directly (without using the Integrality Theorem 9.7) that the complex algebra of a geometry is integral and therefore simple.

9.15. Let $\mathfrak{A}$ be a Boolean algebra with normal operators. A unary discriminator in $\mathfrak{A}$ is a term definable operation c such that

$$c(r) = \begin{cases} 0 & \text{if } r = 0, \\ 1 & \text{if } r \neq 0. \end{cases}$$

Prove that if $\mathfrak{A}$ is non-degenerate and has a unary discriminator, then $\mathfrak{A}$ must be simple.

9.16. A *discriminator term* for an equationally axiomatizable class V of Boolean algebras with normal operators is a term τ with one free variable that defines a unary discriminator (see Exercise 9.8) in every subdirectly irreducible algebra in V. Prove that a term τ is a discriminator term for V if and only if the laws (a)–(d) in Exercise 8.79 (with c replaced everywhere by τ) are valid in V.

9.17. An equationally axiomatizable class of normal Boolean algebras with operators is called a *discriminator variety* if it has a discriminator term (see Exercise 9.16). Prove that in a discriminator variety, the notions of simplicity, subdirect irreducibility, and direct indecomposability coincide.

9.18. Let V be a discriminator variety of Boolean algebras with normal operators (see Exercise 9.17). Prove that for every quantifier-free formula Γ in the first-order language of V, there is a term γ with the same free variables as Γ such that Γ and the equation $\gamma = 0$ are equivalent in all simple algebras in V.

Chapter 10
Relativizations

The notion of a relativization of a relation algebra $\mathfrak{A}$ is closely related to the notion of a subalgebra of $\mathfrak{A}$. In the latter, the fundamental operations of $\mathfrak{A}$ are restricted to a subset of $\mathfrak{A}$ that is closed under these operations. In the former, the fundamental operations of $\mathfrak{A}$ are relativized to the subset of all elements below a given element. Relativizations play a fundamental role in the study of direct decompositions of relation algebras.

10.1 Relativizations to equivalence elements

Consider an arbitrary equivalence element e in a relation algebra $\mathfrak{A}$. The subset

$$A(e) = \{r \in A : r \leq e\} = \{r \cdot e : r \in A\}$$

contains 0 and is easily seen to be closed under the operations of addition, multiplication, converse, and relative multiplication in $\mathfrak{A}$. Indeed, if r and s are elements in $A(e)$, then r and s are both below e, and therefore

$$\begin{aligned} r + s \leq e + e = e, \qquad & r \cdot s \leq e \cdot e = e, \\ r^{\smile} \leq e^{\smile} = e, \qquad & r \,;\, s \leq e \,;\, e = e, \end{aligned}$$

by Boolean algebra, the monotony laws for converse and relative multiplication, and Lemma 5.8(ii). Consequently, the sum, product, converse, and relative product of two elements in $A(e)$ is again an element in $A(e)$.

S. Givant, *Introduction to Relation Algebras*,
DOI 10.1007/978-3-319-65235-1_10

The set $A(e)$ does not contain the identity element, the diversity element, or the unit of $\mathfrak{A}$, but it does contain relativized versions of these elements, namely

$$e \cdot 1', \qquad e \cdot 0', \qquad \text{and} \qquad e \cdot 1$$

(the latter coincides with e, of course). Most importantly, $A(e)$ is not closed under the operation of complement, but it is closed under a relativized version of this operation. The *relativized complement operation* (with respect to e) is the unary operation $-_e$ on $A(e)$ that is defined by

$$-_e r = e - r = e \cdot -r$$

for all elements r in $A(e)$ (where $-r$ is the complement of r in $\mathfrak{A}$). The element $-_e r$ is called the *relative complement* of r (with respect to e).

The *relativization of* $\mathfrak{A}$ *to* e is the algebra

$$\mathfrak{A}(e) = (A(e)\,,+\,,-_e\,,;\,,\smile\,,e \cdot 1').$$

In this notation, we have followed the common algebraic practice of using the same symbols to denote the restricted operations of addition, relative multiplication, and converse in $\mathfrak{A}(e)$ as are used to denote the corresponding operations in $\mathfrak{A}$. The key fact about $\mathfrak{A}(e)$ is that it is a relation algebra.

Theorem 10.1. *The relativization of a relation algebra to an equivalence element is always a relation algebra.*

Proof. Let e be an equivalence element in a relation algebra $\mathfrak{A}$. Every law, that is to say, every equation or implication between equations, that involves only the operations of addition, multiplication, relative multiplication, converse, and zero (but not complement or the identity element) must hold in $\mathfrak{A}(e)$ whenever it holds in $\mathfrak{A}$, because these operations in $\mathfrak{A}(e)$ are just restrictions of the corresponding operations in $\mathfrak{A}$, and zero is the same element in both algebras. From this observation, it follows that Axioms (R1), (R2), (R4), (R6)–(R9), and the implication in (R11) hold in $\mathfrak{A}(e)$.

A short computation using only Boolean laws shows that

$$-_e(-_e r + s) = r \cdot -s \qquad \text{and} \qquad -_e\,(-_e r + -_e s) = r \cdot s$$

for all elements r and s below e. The sum of $r \cdot -s$ and $r \cdot s$ is r, so

$$-_e(-_e r + s) + -_e(-_e r + -_e s) = r.$$

Thus, Axiom (R3) holds in $\mathfrak{A}(e)$.

Turn finally to Axiom (R5). If an element r is below e, then

$$(1 \mathbin{;} r) \cdot 1' \leq (1 \mathbin{;} e) \cdot 1' = e \cdot 1',$$

by the monotony law for relative multiplication and the first dual of Lemma 5.18(ii). Consequently, $r \mathbin{;} (e \cdot 1') = r$, by the first dual of Lemma 5.49 (with e and $e \cdot 1'$ in place of r and x respectively). Thus, Axiom (R5) holds in $\mathfrak{A}(e)$. □

It is time to look at some examples of relativizations. Consider first an arbitrary symmetric, transitive (but not necessarily reflexive) relation E on a set U. The relativization of the full set relation algebra $\mathfrak{Re}(U)$ on the set U to the relation E is just the full set relation algebra $\mathfrak{Re}(E)$ on the equivalence relation E. If E has just one equivalence class V, so that E is the Cartesian square $E = V \times V$, then the relativization of $\mathfrak{Re}(U)$ to E coincides with the full set relation algebra $\mathfrak{Re}(V)$ on the set V.

The next example is a generalization of the preceding one. Consider an arbitrary equivalence relation E on a set U, and an equivalence relation F that is included in E. The relativization of the full set relation algebra $\mathfrak{Re}(E)$ to F coincides with the full set relation algebra $\mathfrak{Re}(F)$. For a concrete instance of this example, take X to be a set of equivalence classes of E. The subrelation

$$F = \bigcup\{V \times V : V \in X\}$$

is an equivalence element in $\mathfrak{Re}(E)$, and the relativization of $\mathfrak{Re}(E)$ to the relation F is the full set relation algebra $\mathfrak{Re}(F)$. Notice that in this case, F is an ideal element in $\mathfrak{Re}(E)$.

For the third example, consider the complex algebra $\mathfrak{Cm}(G)$ of a group G. The non-zero equivalence elements in the algebra $\mathfrak{Cm}(G)$ are just the subgroups of G, and every such equivalence element is reflexive, because the identity element of the group belongs to every subgroup. The relativization of $\mathfrak{Cm}(G)$ to H coincides with the complex algebra $\mathfrak{Cm}(H)$. Notice that the algebra $\mathfrak{Cm}(G)$ is simple, so a subgroup H will not be an ideal element in $\mathfrak{Cm}(G)$ unless H is the improper subgroup.

In a geometric complex algebra $\mathfrak{Cm}(P)$, the non-zero equivalence elements are just the sets of the form $Q \cup \{\iota\}$, where Q is some subspace

of P, and ι is the new element that is adjoined as an identity element to P to form $\mathfrak{Cm}(P)$. Each such non-zero equivalence element $Q \cup \{\iota\}$ is clearly reflexive, and the relativization of $\mathfrak{Cm}(P)$ to $Q \cup \{\iota\}$ is just the algebra $\mathfrak{Cm}(Q)$. As in the case of group complex algebras, the algebra $\mathfrak{Cm}(P)$ is simple, so the equivalence element $Q \cup \{\iota\}$ is not an ideal element unless Q is the improper subspace.

For the last example, consider an arbitrary relation algebra $\mathfrak{A}$, and take e to be a subidentity element in $\mathfrak{A}$. The relativization of $\mathfrak{A}$ to e is a Boolean relation algebra, by Lemmas 5.20(i) and 3.1. In this case, e is usually not an ideal element in $\mathfrak{A}$.

10.2 Relativizations to ideal elements

From the perspective of the algebraic theory, the most important relativizations are to ideal elements. Every ideal element e in a relation algebra $\mathfrak{A}$ is certainly an equivalence element, since

$$e\,;e = e \cdot e = e \qquad \text{and} \qquad e^{\smile} = e,$$

by Lemma 5.41(i),(ii). It therefore makes sense to speak of the relativization of $\mathfrak{A}$ to e. Relativizations to ideal elements can be characterized by an interesting and important homomorphism property.

In a Boolean algebra B, the *relativization mapping* induced by an arbitrary element e is the function φ defined by

$$\varphi(r) = e \cdot r,$$

for every element r in B. This mapping is always a complete Boolean epimorphism from B onto the Boolean relativization $B(e)$. Indeed, each element below e is mapped to itself by φ, so φ is certainly onto. For every element r in B, we have

$$\varphi(-r) = e \cdot -r = e \cdot -(e \cdot r) = -_e\varphi(r),$$

by the definition of φ, the definition of complement in a Boolean relativization, and by Boolean algebra, so φ preserves the operation of complement. And for every subset X of B that has a supremum r, we have

$$\varphi(r) = e \cdot r = e \cdot (\sum X) = \sum\{e \cdot s : s \in X\} = \sum\{\varphi(s) : s \in X\},$$

by the complete distributivity of multiplication, so φ preserves all sums that exist in B.

In a relation algebra, it is no longer the case that the relativization mapping induced by an equivalence element e is always a homomorphism. In fact, this mapping is a homomorphism if and only if e is an ideal element.

Theorem 10.2. *Let e be an arbitrary element in a relation algebra $\mathfrak{A}$, and let φ be the relativization mapping defined by*

$$\varphi(r) = e \cdot r$$

for all elements r in $\mathfrak{A}$. If e is an ideal element, then φ is a complete epimorphism from $\mathfrak{A}$ to the relativization $\mathfrak{A}(e)$. Conversely, if φ is a homomorphism, then e is an ideal element.

Proof. As has already been observed, the relativization mapping φ is always a complete Boolean epimorphism from the Boolean part of $\mathfrak{A}$ into the Boolean part of the relativization $\mathfrak{A}(e)$. In order for φ to be a relation algebraic epimorphism, it is necessary and sufficient that φ preserve the operation of relative multiplication, by the remarks preceding Lemma 7.7. To say that φ preserves relative multiplication means that

$$\varphi(r\,;s) = \varphi(r)\,;\varphi(s)$$

for all elements r and s in $\mathfrak{A}$. In view of the definition of φ, this amounts to the requirement that

$$e \cdot (r\,;s) = (e \cdot r)\,;(e \cdot s)$$

for all elements r and s in $\mathfrak{A}$. In other words, the distributive law for multiplication over relative multiplication must hold for e. The validity of this law characterizes ideal elements, by Lemma 5.44, so φ preserves relative multiplication if and only if e is an ideal element. □

If e is an ideal element in $\mathfrak{A}$, then the relativization $\mathfrak{A}(e)$ is a homomorphic image of $\mathfrak{A}$, by the previous theorem, and therefore must be isomorphic to the quotient of $\mathfrak{A}$ modulo some ideal, by the First Isomorphism Theorem 8.39. It is a natural and important problem to determine what that ideal is.

Theorem 10.3. *If e is an ideal element in a relation algebra $\mathfrak{A}$, and if φ is the relativization mapping induced by e, then the kernel of φ is the principal ideal $(-e)$, and the relativization $\mathfrak{A}(e)$ is isomorphic to the quotient algebra $\mathfrak{A}/(-e)$ via the function that maps each element r in $\mathfrak{A}(e)$ to the coset $r/(-e)$.*

Proof. The kernel of φ is, by definition, the set of elements that are mapped to zero by φ. The definition of φ as the relativization mapping implies that this kernel must be the set of elements that are disjoint from e, or put another way, it must be the set of elements that are below $-e$. This set is, of course, just the principal ideal $(-e)$. Recall, in this connection, that $-e$ is also an ideal element, by Lemma 5.39(iv).

The mapping φ is an epimorphism from $\mathfrak{A}$ to the relativization $\mathfrak{A}(e)$, by Theorem 10.2. Apply the First Isomorphism Theorem to conclude that the quotient of $\mathfrak{A}$ modulo the kernel of φ is isomorphic to $\mathfrak{A}(e)$ via the mapping that takes each coset $r/(-e)$ to the element $\varphi(r)$. In other words, the isomorphism maps $r/(-e)$ to $e \cdot r$, by the definition of φ. The elements in $\mathfrak{A}(e)$ are precisely the elements in $\mathfrak{A}$ that are below e, so the inverse isomorphism maps each element r in $\mathfrak{A}(e)$ to the coset $r/(-e)$. □

10.3 Properties preserved under relativizations

There are a number of important properties that are easily seen to be preserved under the passage to relativizations. For example, the relativization of a subalgebra is a subalgebra of the relativization, the relativization of a homomorphic image is a homomorphic image of the relativization, and the relativization of an ideal is an ideal in the relativization. Here is a precise statement of these assertions.

Lemma 10.4. *Let e be an equivalence element in a relation algebra $\mathfrak{A}$.*

(i) *If $\mathfrak{B}$ is a subalgebra of $\mathfrak{A}$ that contains e, then $\mathfrak{B}(e)$ is a subalgebra of $\mathfrak{A}(e)$.*
(ii) *If $\mathfrak{B}$ is a regular subalgebra of $\mathfrak{A}$ that contains e, then $\mathfrak{B}(e)$ is a regular subalgebra of $\mathfrak{A}(e)$.*
(iii) *If φ is a homomorphism from $\mathfrak{A}$ into $\mathfrak{B}$, and if $f = \varphi(e)$, then the restriction of φ to $\mathfrak{A}(e)$ is a homomorphism from $\mathfrak{A}(e)$ into $\mathfrak{B}(f)$. Moreover, if φ is one-to-one or onto, then the restriction of φ is also one-to-one or onto respectively.*

(iv) *If M is an ideal in $\mathfrak{A}$, then the intersection $M \cap A(e)$ is an ideal in $\mathfrak{A}(e)$, and this intersection is equal to the set $\{r \cdot e : r \in M\}$.*

Proof. Suppose $\mathfrak{B}$ is a subalgebra of $\mathfrak{A}$. The operations of addition, relative multiplication, and converse in $\mathfrak{B}(e)$ and in $\mathfrak{A}(e)$ are just the appropriate restrictions of the corresponding operations of $\mathfrak{B}$ and $\mathfrak{A}$ respectively, by the remarks in Section 10.1. Since the operations in $\mathfrak{B}$ are also restrictions of the corresponding operations in $\mathfrak{A}$, it follows that the operations of addition, relative multiplication, and converse in the relativization $\mathfrak{B}(e)$ are restrictions of the corresponding operations in the relativization $\mathfrak{A}(e)$. In both relativizations, the complement of an element r from $\mathfrak{B}(e)$ is just $e \cdot -r$, where the complement $-r$ is formed in $\mathfrak{B}$ or in $\mathfrak{A}$ (since the operation of forming complements in $\mathfrak{B}$ is the restriction of the corresponding operation in $\mathfrak{A}$). Consequently, the complement operation in $\mathfrak{B}(e)$ is the restriction of the complement operation in $\mathfrak{A}(e)$. Finally, the identity element in both relativizations is $e \cdot 1'$, where 1' is the identity element in $\mathfrak{B}$ and in $\mathfrak{A}$, so the two relativizations have the same identity element. Conclusion: $\mathfrak{B}(e)$ is a subalgebra of $\mathfrak{A}(e)$. This proves (i).

Part (ii) follows from (i) and the following observation. If a subset X of the relativization $\mathfrak{B}(e)$ has a supremum r in $\mathfrak{B}(e)$, then r remains the supremum of X in $\mathfrak{B}$. The algebra $\mathfrak{B}$ is assumed to be a regular subalgebra of $\mathfrak{A}$, so r is the supremum of X in $\mathfrak{A}$, and therefore it is the supremum of X in $\mathfrak{A}(e)$.

Assume next that φ is a homomorphism from $\mathfrak{A}$ into $\mathfrak{B}$. Observe that the image $f = \varphi(e)$ must be an equivalence element in $\mathfrak{B}$, by Lemma 7.2 (see also the remarks following Corollary 7.3), so it makes sense to speak of the relativization of $\mathfrak{B}$ to f. As has already been noted, the operations of addition, relative multiplication, and converse in the relativizations $\mathfrak{A}(e)$ and $\mathfrak{B}(f)$ are restrictions of the corresponding operations in the algebras $\mathfrak{A}$ and $\mathfrak{B}$ respectively. Since φ is assumed to preserve these operations in the latter algebras, it must preserve these operations in the relativizations. The proof that φ preserves the operation of forming relativized complements is equally easy: if r is an element in $\mathfrak{A}(e)$, then

$$\varphi(-_e r) = \varphi(e - r) = \varphi(e) - \varphi(r) = f - \varphi(r) = -_f \varphi(r).$$

Finally, φ maps the element $e \cdot 1'$ in $\mathfrak{A}(e)$ to the element $f \cdot 1'$ in $\mathfrak{B}(f)$, so it preserves the relativized identity element. Conclusion: the restriction of φ to $\mathfrak{A}(e)$ is indeed a homomorphism from $\mathfrak{A}(e)$ into $\mathfrak{B}(f)$.

Clearly, if φ is one-to-one, then so is its restriction. If φ happens to be onto, then in particular, every element s in $\mathfrak{B}(f)$ is the image under φ of some element r in $\mathfrak{A}$. The element $e \cdot r$ belongs to $\mathfrak{A}(e)$, and

$$\varphi(e \cdot r) = \varphi(e) \cdot \varphi(r) = f \cdot s = s,$$

by the homomorphism properties of φ and the fact that the element s is below f. Consequently, the restriction of φ is onto.

Turn now to the proof of (iv). The definition of an ideal involves only the element zero and the operations of addition, multiplication, and relative multiplication. These operations in the relativization $\mathfrak{A}(e)$ are all restrictions of the corresponding operations in $\mathfrak{A}$, so the intersection of an ideal in $\mathfrak{A}$ with the set $A(e)$ must be an ideal in $\mathfrak{A}(e)$. To give a concrete example of how the argument proceeds, consider condition (ii) in the definition of an ideal. If M is an ideal in $\mathfrak{A}$, and if r and s are elements in $M \cap A(e)$, then r and s are in both M and $A(e)$, by the definition of intersection, and therefore the sum $r + s$ is in both M and $A(e)$, because M (as an ideal) and $A(e)$ are closed under the operation of addition in $\mathfrak{A}$. It follows that $r + s$ belongs to $M \cap A(e)$.

To prove the final assertion in (iv), write

$$N = \{r \cdot e : r \in M\}, \tag{1}$$

with the goal of showing that

$$N = M \cap A(e). \tag{2}$$

If s belongs to the right side of (2), then s is in M and also below e, so that $s = s \cdot e$. Therefore, s belongs to the left side of (2), by (1). On the other hand, if s belongs to the left side of (2), then s has the form $s = r \cdot e$ for some r in M, by (1), so s is certainly in $A(e)$. Also, s is below r and therefore in M, by condition (v) in Lemma 8.8. Consequently, s belongs to the right side of (2). Thus, (2) holds. □

The property of a relation algebra $\mathfrak{A}$ being atomic is also preserved under the passage to relativizations.

Lemma 10.5. *Let e be an equivalence element in a relation algebra $\mathfrak{A}$. An element $r \leq e$ is an atom in $\mathfrak{A}(e)$ if and only if r is an atom in $\mathfrak{A}$. Consequently, if $\mathfrak{A}$ is atomic, then so is $\mathfrak{A}(e)$.*

Proof. An atom r is, by definition, a minimal non-zero element. This definition involves only the elements that are below r, so for elements

that are below e, the definition of an atom has the same meaning in $\mathfrak{A}(e)$ as it does in $\mathfrak{A}$. Thus, the atoms in $\mathfrak{A}(e)$ are just the atoms in $\mathfrak{A}$ that are below e. In particular, if every non-zero element in $\mathfrak{A}$ is above an atom in $\mathfrak{A}$, then in particular every non-zero element that is below e is above an atom in $\mathfrak{A}$, and that atom must belong to $\mathfrak{A}(e)$. In other words, if $\mathfrak{A}$ is atomic, then so is $\mathfrak{A}(e)$. □

Yet another property that is preserved under the passage to relativizations is completeness.

Lemma 10.6. *Let e be an equivalence element in a relation algebra $\mathfrak{A}$. A subset X of $\mathfrak{A}(e)$ has a supremum in $\mathfrak{A}(e)$ if and only if it has a supremum in $\mathfrak{A}$, and when these suprema exist, they are equal. Consequently, if $\mathfrak{A}$ is complete, then so is $\mathfrak{A}(e)$.*

Proof. The element e is obviously an upper bound of the set X (in both $\mathfrak{A}(e)$ and $\mathfrak{A}$). The existence or non-existence of a supremum of X therefore depends only on the elements that are below e, so the notion of supremum when applied to X must yield the same result in $\mathfrak{A}(e)$ as it does in $\mathfrak{A}$.

In more detail, if an element s in $\mathfrak{A}$ is an upper bound of the set X in $\mathfrak{A}$, then the product $e \cdot s$ is an upper bound of X that is below s and belongs to $\mathfrak{A}(e)$. Thus, every upper bound of X in $\mathfrak{A}$ is above an upper bound of X in $\mathfrak{A}(e)$. Consequently, in looking for a smallest element in the set of upper bounds of X in $\mathfrak{A}$, we need only consider those elements that are already in $\mathfrak{A}(e)$. If r is the supremum of X in $\mathfrak{A}$, then r must belong to $\mathfrak{A}(e)$, by the preceding observations, and therefore r must be the supremum of X in $\mathfrak{A}(e)$. Conversely, if r is the supremum of X in $\mathfrak{A}(e)$, then r is below every upper bound of X in $\mathfrak{A}$, by the preceding observations, and therefore r is the supremum of X in $\mathfrak{A}$.

If every subset of $\mathfrak{A}$ has a supremum in $\mathfrak{A}$, then in particular every subset of $\mathfrak{A}(e)$ has a supremum in $\mathfrak{A}$, and that supremum remains the supremum of the subset in $\mathfrak{A}(e)$. In other words, if $\mathfrak{A}$ is complete, then so is $\mathfrak{A}(e)$. □

The examples at the end of Section 10.1 suggest that the property of being integral might be preserved under the passage to relativizations, and with one obvious exception, this proves to be the case.

Lemma 10.7. *A non-zero equivalence element e in an integral relation algebra $\mathfrak{A}$ is always reflexive, and the relativization $\mathfrak{A}(e)$ is integral.*

Proof. The identity element 1' is an atom in $\mathfrak{A}$, by the Integrality Theorem 9.7. The relativized identity element $e \cdot 1'$ is non-zero, by Corollary 5.19 and the assumption that e is non-zero, so the atom 1' must be below e. It follows that e is reflexive and 1' is the identity element in $\mathfrak{A}(e)$. Use Lemma 10.5 to conclude that 1' is an atom in $\mathfrak{A}(e)$, and therefore $\mathfrak{A}(e)$ is integral, by Theorem 9.7 applied to $\mathfrak{A}(e)$. □

One other observation of a positive character is worth mentioning. Part (vi) of Lemma 5.48 says that when an element r is below an equivalence element e, the computation of the domain and range of r in $\mathfrak{A}(e)$ and in $\mathfrak{A}$ leads to the same results. Consequently, when a rectangle and its sides are below e, it does not matter in Lemma 5.59 and Corollary 5.60 whether the domains and ranges are computed in $\mathfrak{A}(e)$ or in $\mathfrak{A}$.

10.4 Relativizations and simple algebras

Not all properties are preserved under the passage to relativizations. An important example is the property of simplicity. We have already seen that if E is an equivalence relation on a set U, and if E has more than one equivalence class, then the relativization of the simple relation algebra $\mathfrak{Re}(U)$ to the equivalence relation E is the non-simple relation algebra $\mathfrak{Re}(E)$. In fact, it is known (see [34]) that every relation algebra is a relativization of a simple relation algebra to an equivalence element.

In view of the failure of simplicity to be preserved under the passage to relativizations, it becomes especially important to find conditions under which the relativization of a simple relation algebra to an equivalence element does remain simple. One condition is that the element be a non-zero square. Note that every square is an equivalence element, by Lemma 5.64, and a square is non-zero if and only if the side of the square is non-zero (see Exercise 5.39).

Lemma 10.8. *The relativization of a simple relation algebra to a non-zero square is always simple.*

Proof. Consider a non-zero square $e = x\,;1\,;x$ with side x in a simple relation algebra $\mathfrak{A}$. The identity element in the relativization $\mathfrak{A}(e)$ is the element $e \cdot 1'$, by definition. Since this element coincides with x, by

Lemma 5.18(iii) (with x in place of r), it follows that x is the identity element in $\mathfrak{A}(e)$. Consequently,

$$x \,;\, r = r \,;\, x = r \tag{1}$$

for every element r in $\mathfrak{A}(e)$.

Consider now an arbitrary non-zero element r in $\mathfrak{A}(e)$. We have

$$\begin{aligned} e \,;\, r \,;\, e = (x \,;\, 1 \,;\, x) \,;\, r \,;\, (x \,;\, 1 \,;\, x) &= x \,;\, (1 \,;\, x \,;\, r \,;\, x \,;\, 1) \,;\, x \\ &= x \,;\, (1 \,;\, r \,;\, 1) \,;\, x = x \,;\, 1 \,;\, x = e, \end{aligned}$$

by the assumption about e, the associative law for relative multiplication, (1), the assumption that $\mathfrak{A}$ is simple, and the Simplicity Theorem 9.2. Since e is the unit of $\mathfrak{A}(e)$, and since e is non-zero by assumption, it follows from the preceding computation and Theorem 9.2 (with 1 replaced by e) that $\mathfrak{A}(e)$ is simple. □

It turns out that relativizations of arbitrary relation algebras (and not just of simple relation algebras) to ideal element atoms are always simple. To prove this, it is helpful to determine first the ideal elements in a relativization.

Lemma 10.9. *If e is an ideal element in a relation algebra $\mathfrak{A}$, then the ideal elements in the relativization $\mathfrak{A}(e)$ are exactly the ideal elements in $\mathfrak{A}$ that are below e. In particular, the ideal element atoms in $\mathfrak{A}(e)$ are exactly the ideal element atoms in $\mathfrak{A}$ that are below e.*

Proof. Every ideal element r in $\mathfrak{A}$ that is below e remains an ideal element in $\mathfrak{A}(e)$, because

$$e \,;\, r \,;\, e = e \cdot r \cdot e = r,$$

by Lemma 5.41(ii) and Boolean algebra. On the other hand, if r is an ideal element in $\mathfrak{A}(e)$, then $e \,;\, r \,;\, e = r$, by the definition of an ideal element in $\mathfrak{A}(e)$, and therefore

$$1 \,;\, r \,;\, 1 = 1 \,;\, e \,;\, r \,;\, e \,;\, 1 = e \,;\, r \,;\, e = r,$$

by the assumption that e is an ideal element and Lemma 5.38(vi). Consequently, r is an ideal element in $\mathfrak{A}$ that is below e. This proves the first assertion of the lemma.

The second assertion of the lemma is an easy consequence of the first assertion and is proved in a manner analogous to the proof of the first part of Lemma 10.5. □

Corollary 10.10. *For the relativization of a relation algebra* $\mathfrak{A}$ *to an ideal element* e *to be simple*, *it is necessary and sufficient that* e *be an ideal element atom in* $\mathfrak{A}$.

Proof. The relativization $\mathfrak{A}(e)$ is simple if and only if e is an ideal element atom in $\mathfrak{A}(e)$, by Lemma 9.1 (see the remark following the lemma). In view of Lemma 10.9, this last condition is equivalent to the condition that e be an ideal element atom in $\mathfrak{A}$. □

If an element r is an atom, then the generated ideal element $1 ; r ; 1$ is an ideal element atom, by Lemma 8.28. This gives the following consequence of Corollary 10.10.

Corollary 10.11. *If* r *is an atom in a relation algebra* $\mathfrak{A}$, *then the relativization* $\mathfrak{A}(1 ; r ; 1)$ *is simple*.

10.5 Generalized relativizations

Theorem 10.3 implies that relativizations to ideal elements capture only some of the homomorphic images of a relation algebra $\mathfrak{A}$, namely those images that, up to isomorphism, can also be realized as quotients of $\mathfrak{A}$ by principal ideals. We shall see in Theorem 14.54 that if one is willing to broaden the notion of a relativization, then every homomorphic image of $\mathfrak{A}$ can be realized as a relativization of $\mathfrak{A}$ to an ideal element.

To define this broader notion, suppose $\mathfrak{B}$ is a subalgebra of a relation algebra $\mathfrak{A}$, and consider an ideal element e in $\mathfrak{A}$ that may or may not belong to $\mathfrak{B}$. The relativization epimorphism induced on $\mathfrak{A}$ by e maps the set B onto the set

$$B(e) = \{e \cdot r : r \in B\}.$$

Since B is a subuniverse of $\mathfrak{A}$, the homomorphic image set $B(e)$ must be a subuniverse of $\mathfrak{A}(e)$, by Lemma 7.4. The corresponding subalgebra is called the (*generalized*) *relativization of* $\mathfrak{B}$ *to* e, and is denoted by $\mathfrak{B}(e)$. We shall also occasionally refer to $\mathfrak{B}(e)$ as a *relativized subalgebra* of $\mathfrak{A}$. The unit in $\mathfrak{B}(e)$ is the element e, the identity element in $\mathfrak{B}(e)$ is the relativized identity element $e \cdot 1'$, and the complement of an element $e \cdot r$ in $\mathfrak{B}(e)$ is the relativized complement $e \cdot -r$, where $-r$ is the complement of r in $\mathfrak{A}$ and in $\mathfrak{B}$. The remaining operations of $\mathfrak{B}(e)$

are just restrictions of the corresponding operations of $\mathfrak{A}$. Warning: in general, the set $B(e)$ is not a subset of $\mathfrak{B}$, and in particular it does *not* coincide with the set of elements in $\mathfrak{B}$ that are below e. In fact, if e is not in $\mathfrak{B}$, then at least half of the elements in $B(e)$ do not belong to $\mathfrak{B}$ at all, since for each element r in $\mathfrak{B}$, the presence of both $e \cdot r$ and its relative complement $e \cdot -r$ in $\mathfrak{B}$ would imply that their sum, which is e, is also in $\mathfrak{B}$. For this reason, it would be incorrect to refer to the remaining operations of $\mathfrak{B}(e)$ as restrictions of the corresponding operations of $\mathfrak{B}$.

The observations made so far may be summarized as follows.

Lemma 10.12. *If $\mathfrak{B}$ is a subalgebra of a relation algebra $\mathfrak{A}$, and if e is an ideal element in $\mathfrak{A}$, then the relativization $\mathfrak{B}(e)$ is a relation algebra. In fact, $\mathfrak{B}(e)$ is a subalgebra of $\mathfrak{A}(e)$ and also a homomorphic image of $\mathfrak{B}$ under the relativization mapping on $\mathfrak{A}$ that is induced by e.*

It is important for later use to determine the ideal elements in the generalized relativization $\mathfrak{B}(e)$. As it turns out, an analogue of Lemma 10.9 holds.

Lemma 10.13. *If $\mathfrak{B}$ is a subalgebra of a relation algebra $\mathfrak{A}$, and if e is an ideal element in $\mathfrak{A}$, then the ideal elements in $\mathfrak{B}(e)$ are just the relativizations to e of the ideal elements in $\mathfrak{B}$.*

Proof. If s is an ideal element in $\mathfrak{B}$, then s is also an ideal element in $\mathfrak{A}$, and therefore the product $r = e \cdot s$ is an ideal element in $\mathfrak{A}$, by Lemma 5.39(iii). Since

$$e \,;\, r \,;\, e = e \cdot r \cdot e = e \cdot (e \cdot s) \cdot e = e \cdot s = r$$

in $\mathfrak{A}$, and therefore also in $\mathfrak{B}(e)$, by Lemma 5.41(ii), Boolean algebra, and the definition of r, it follows that r is an ideal element in $\mathfrak{B}(e)$. (In this connection, recall that multiplication and relative multiplication in $\mathfrak{B}(e)$ are the restrictions of the corresponding operations in $\mathfrak{A}$.) This proves that relativizations to e of ideal elements in $\mathfrak{B}$ are ideal elements in $\mathfrak{B}(e)$.

To prove the converse, suppose that r is an ideal element in $\mathfrak{B}(e)$. There must be an element t in $\mathfrak{B}$ such that $r = e \cdot t$, by the definition of $\mathfrak{B}(e)$. The element $s = 1 \,;\, t \,;\, 1$ is certainly an ideal element in $\mathfrak{B}$, by Lemma 5.38, and

$$e \cdot s = e \cdot (1 \,;\, t \,;\, 1) = (e \cdot 1) \,;\, (e \cdot t) \,;\, (e \cdot 1) = e \,;\, r \,;\, e = r,$$

by the definition of s, the assumption that e is an ideal element in $\mathfrak{A}$ and Lemma 5.44 (with e in place of r), the choice of t, and the assumption that r is an ideal element in $\mathfrak{B}(e)$. Consequently, r is the relativization to e of an ideal element in $\mathfrak{B}$, namely the ideal element s. $\square$

If a relation algebra $\mathfrak{B}$ is simple, then its only ideal elements are 0 and 1, so the only ideal elements in $\mathfrak{B}(e)$ are 0 and e, by the preceding lemma. Thus, for non-zero ideal elements e, the relativization $\mathfrak{B}(e)$ must be simple.

Corollary 10.14. *If $\mathfrak{B}$ is a simple subalgebra of a* (*not necessarily simple*) *relation algebra $\mathfrak{A}$, and if e is a non-zero ideal element in $\mathfrak{A}$, then $\mathfrak{B}(e)$ is simple.*

10.6 Historical remarks

The notion of a relativization of a relation algebra was already studied by Tarski in [105], where it is stated that the relativization of a relation algebra to an equivalence relation is a relation algebra. A statement of this theorem is also given informally in [55].

The first part of Theorem 10.2, asserting that the relativization mapping induced by an ideal element e in a relation algebra $\mathfrak{A}$ is an epimorphism from $\mathfrak{A}$ to $\mathfrak{A}(e)$, is stated and proved in Jónsson-Tarski [55]. The second part of the theorem, asserting that this property characterizes ideal elements, was probably known to Tarski at that time, because it is based on the characterization of ideal elements in Lemma 5.44, which is already given in [105]. At any rate, this second part is stated explicitly in [112]. The description in Theorem 10.3 of relativizations to ideal elements in terms of quotients modulo principal ideals seems to be due to Tarski. It was given in the lectures [112], but it probably dates from an earlier period.

The results in Sections 10.3–10.5 are due to Givant, and many of them occur in [34]. In more detail, part (i) of Lemma 10.4 is from [34], but this result was also obtained independently and earlier by Maddux in [74]. Part (iii) of Lemma 10.4 is from [34], as are Lemmas 10.5, 10.8, and 10.9, and Corollaries 10.10 and 10.11. As is mentioned in [34], Lemma 10.8 and Corollary 10.11 were discovered independently about the same time by Peter Jipsen. The notion of a generalized relativization, and the results given in Section 10.5, are all from [34].

More general notions of relativizations of relation algebras have been studied by Maddux [74], Richard Kramer [60], and Maarten Marx [80].

Exercises

10.1. Show that an arbitrary element e in a Boolean relation algebra $\mathfrak{A}$ is an equivalence element. Describe the relativization $\mathfrak{A}(e)$.

10.2. What are the non-zero equivalence elements in the complex algebra of a modular lattice L with zero? Describe the relativizations of $\mathfrak{Cm}(L)$ to its non-zero equivalence elements.

10.3. Prove directly, without using the remarks preceding Lemma 7.7, that the relativization mapping in Theorem 10.2 preserves the operation of converse and maps the identity element in $\mathfrak{A}$ to the identity element in $\mathfrak{A}(e)$.

10.4. If N is an ideal in a relativization $\mathfrak{A}(e)$, is there necessarily an ideal M in $\mathfrak{A}$ such that $N = M \cap A(e)$?

10.5. Let e be an ideal element in a relation algebra $\mathfrak{A}$. If a set X generates $\mathfrak{A}$, prove that the relativized set

$$Y = \{e \cdot r : r \in X\}$$

generates $\mathfrak{A}(e)$. Does this remain true if e is an arbitrary equivalence element?

10.6. Is it true for an arbitrary equivalence element e in a relation algebra $\mathfrak{A}$ that the ideal elements in $\mathfrak{A}(e)$ are precisely the elements of the form $e \cdot r$, where r ranges over the ideal elements in $\mathfrak{A}$? In other words, are the ideal elements in $\mathfrak{A}(e)$ just the relativizations to e of the ideal elements in $\mathfrak{A}$?

10.7. Prove the second assertion of Lemma 10.9.

10.8. Derive Corollary 10.10 directly from Theorem 10.3, without using Lemma 10.9.

10.9. Suppose $\mathfrak{B}$ is the Boolean relation algebra of finite and cofinite subsets of an infinite set U, and $\mathfrak{A}$ the Boolean relation algebra of all subsets of U. For an arbitrary element E in $\mathfrak{A}$, describe the generalized relativization $\mathfrak{B}(E)$. What if E is an infinite subset of U whose complement is also an infinite subset of U?

10.10. Suppose $\mathfrak{B}$ is a subalgebra of a relation algebra $\mathfrak{A}$, and e is an ideal element in $\mathfrak{A}$ (that may or may not be in $\mathfrak{B}$). Prove that if r is an atom in $\mathfrak{B}$ that is not disjoint from e, then $e \cdot r$ is an atom in $\mathfrak{B}(e)$. Conclude that if $\mathfrak{B}$ is atomic, then so is $\mathfrak{B}(e)$.

10.11. Suppose $\mathfrak{B}$ is a subalgebra of a relation algebra $\mathfrak{A}$, and e an ideal element in $\mathfrak{A}$ (that may or may not be in $\mathfrak{B}$). Prove that the set M of elements in $\mathfrak{B}$ that are disjoint from e (in $\mathfrak{A}$) is an ideal in $\mathfrak{B}$, and that the relativization $\mathfrak{B}(e)$ is isomorphic to the quotient $\mathfrak{A}/M$ via the correspondence that maps $e \cdot r$ to r/M for each r in $\mathfrak{B}$.

10.12. Let e be an ideal element, and f an equivalence element, in a relation algebra $\mathfrak{A}$.

(i) Prove that the relativization mapping φ induced by e—which is an epimorphism from $\mathfrak{A}$ to $\mathfrak{A}(e)$—restricts to an epimorphism from $\mathfrak{A}(f)$ to $\mathfrak{A}(e \cdot f)$.
(ii) If $\mathfrak{B}$ is a subalgebra of the relativization $\mathfrak{A}(f)$, prove that the image of the universe of $\mathfrak{B}$ under the mapping φ is the set

$$B(e) = \{e \cdot r : r \in B\}.$$

(iii) Conclude that $B(e)$ is a subuniverse of $\mathfrak{A}(e \cdot f)$ and the corresponding subalgebra $\mathfrak{B}(e)$ is a homomorphic image of $\mathfrak{B}$ under φ.

10.13. Define a general notion of the relativization of a relation algebra $\mathfrak{A}$ to an arbitrary element e in $\mathfrak{A}$ (so e may not be an equivalence element).

Chapter 11
Direct products

A familiar way of making one new structure out of two old ones is to form their Cartesian product and, in case the structure involves some algebraic operations, to define the requisite operations coordinatewise. Relation algebras furnish an instance of this procedure. For relation algebras, products come in two flavors: the standard Cartesian (or external) product and an internal version of this product. These two versions are but two sides of the same coin, but each has its own advantages and disadvantages. Products form a critical component in the analysis of relation algebras, and in particular in the reduction of the analysis of complicated algebras to that of simple ones.

11.1 Binary external products

The *direct product* of two relation algebras $\mathfrak{B}$ and $\mathfrak{C}$ is the algebra

$$\mathfrak{A} = \mathfrak{B} \times \mathfrak{C},$$

of the same similarity type as relation algebras, in which the universe is the set of the pairs (r, s) with r in $\mathfrak{B}$ and s in $\mathfrak{C}$, and the operations and the identity element are defined coordinatewise, that is to say, they are defined by

$$(r, s) + (t, u) = (r + t, s + u), \qquad -(r, s) = (-r, -s),$$
$$(r, s) ; (t, u) = (r ; t, s ; u), \qquad (r, s)^{\smile} = (r^{\smile}, s^{\smile})$$

for all pairs (r, s) and (t, u) in $\mathfrak{A}$, and $1' = (1', 1')$. (In each of these equations, the first occurrence of the operation or distinguished element is

S. Givant, *Introduction to Relation Algebras*,
DOI 10.1007/978-3-319-65235-1_11

the one being defined in $\mathfrak{A}$, while the second is the corresponding one in $\mathfrak{B}$, and the third is the corresponding one in $\mathfrak{C}$. For instance, in the first equation, $(r,s)+(t,u)$ is a sum in $\mathfrak{A}$, while $r+t$ and $s+u$ are sums in $\mathfrak{B}$ and $\mathfrak{C}$ respectively.) The algebras $\mathfrak{B}$ and $\mathfrak{C}$ are called the *direct factors* of the product $\mathfrak{A}$.

The direct product $\mathfrak{A}$ defined above is often called the *Cartesian product*, or the *external product*, of $\mathfrak{B}$ and $\mathfrak{C}$, in order to distinguish it from an internal product of $\mathfrak{B}$ and $\mathfrak{C}$ that will be defined in Section 11.4. In harmony with this terminology, one can also call $\mathfrak{B}$ and $\mathfrak{C}$ the *Cartesian factors*, or the *external factors* of $\mathfrak{A}$. In order to simplify the terminology, we shall usually refer to $\mathfrak{A}$ as the *product* of $\mathfrak{B}$ and $\mathfrak{C}$, and to $\mathfrak{B}$ and $\mathfrak{C}$ as the *factors* of $\mathfrak{A}$.

11.2 Properties preserved under binary products

The operations of multiplication and relative addition, the distinguished constants zero, one, and the diversity element, and the partial ordering relation in the product $\mathfrak{A} = \mathfrak{B} \times \mathfrak{C}$ are also determined coordinatewise as follows:

$$(r,s)\cdot(t,u) = (r\cdot t, s\cdot u), \qquad (r,s) \mathbin{+\!\!,} (t,u) = (r \mathbin{+\!\!,} t, s \mathbin{+\!\!,} u),$$

$$0 = (0,0), \qquad 1 = (1,1), \qquad 0' = (0', 0'),$$

$$(r,s) \leq (t,u) \qquad \text{if and only if} \qquad r \leq t \text{ and } s \leq u.$$

This observation is an easy consequence of the definitions of these operations and elements in terms of the fundamental operations of $\mathfrak{A}$.

More generally, any operation on the universe of $\mathfrak{A}$ that can be defined by means of a term in the language of relation algebras is performed coordinatewise. To state this result precisely, it is helpful to introduce some terminology. If

$$t = ((r_0, s_0), \dots, (r_{n-1}, s_{n-1}))$$

is a sequence of elements in $\mathfrak{A}$, then the sequences

$$r = (r_0, \dots, r_{n-1}) \qquad \text{and} \qquad s = (s_0, \dots, s_{n-1})$$

in the factor algebras $\mathfrak{B}$ and $\mathfrak{C}$ are called the *left* and *right coordinate sequences* of t respectively, and t is called the *product sequence* of r and s.

Lemma 11.1. *Let* $\gamma(v_0, \ldots, v_{n-1})$ *be a term in the language of relation algebras, and* t *a sequence of* n *elements in a direct product*

$$\mathfrak{A} = \mathfrak{B} \times \mathfrak{C}.$$

If r *and* s *are the left and right coordinate sequences of* t, *then*

$$\gamma^{\mathfrak{A}}(t) = (\gamma^{\mathfrak{B}}(r), \gamma^{\mathfrak{C}}(s)).$$

Proof. Suppose r, s, and t are as hypothesized in the statement of the lemma, and observe that the ith coordinate of t is equal to the pair consisting of the ith coordinates of r and s, in symbols,

$$t_i = (r_i, s_i). \tag{1}$$

The proof that γ is evaluated coordinatewise on t proceeds by induction on terms. There are two base cases to consider. If γ is a variable v_i, then

$$\gamma^{\mathfrak{A}}(t) = t_i = (r_i, s_i) = (\gamma^{\mathfrak{B}}(r), \gamma^{\mathfrak{C}}(s)),$$

by the definition of the value of a term on a sequence of elements in an algebra (see Section 2.4) and (1). A similar argument applies if γ is the distinguished constant 1’.

Assume now as the induction hypothesis that σ and τ are terms whose values on t are determined by

$$\sigma^{\mathfrak{A}}(t) = (\sigma^{\mathfrak{B}}(r), \sigma^{\mathfrak{C}}(s)) \qquad \text{and} \qquad \tau^{\mathfrak{A}}(t) = (\tau^{\mathfrak{B}}(r), \tau^{\mathfrak{C}}(s)). \tag{2}$$

There are four cases to consider. If γ is the term $\sigma ; \tau$, then

$$\begin{aligned}
\gamma^{\mathfrak{A}}(t) &= (\sigma ; \tau)^{\mathfrak{A}}(t) \\
&= \sigma^{\mathfrak{A}}(t) ; \tau^{\mathfrak{A}}(t) \\
&= (\sigma^{\mathfrak{B}}(r), \sigma^{\mathfrak{C}}(s)) ; (\tau^{\mathfrak{B}}(r), \tau^{\mathfrak{C}}(s)) \\
&= (\sigma^{\mathfrak{B}}(r) ; \tau^{\mathfrak{B}}(r), \sigma^{\mathfrak{C}}(s) ; \tau^{\mathfrak{C}}(s)) \\
&= ((\sigma ; \tau)^{\mathfrak{B}}(r), (\sigma ; \tau)^{\mathfrak{C}}(s)) \\
&= (\gamma^{\mathfrak{B}}(r), \gamma^{\mathfrak{C}}(s)).
\end{aligned}$$

The first and last equalities use the assumption on γ, and the second and fifth use the definition of the value of a term on a sequence of elements in an algebra. The third equality uses the induction hypotheses in (2), and the fourth uses the fact that the operation $;$ in $\mathfrak{A}$ is defined

coordinatewise in terms of the corresponding operations in $\mathfrak{B}$ and in $\mathfrak{C}$. Thus, the conclusion of the lemma holds in this case. A similar argument applies if γ is one of the terms $\sigma + \tau$, or $-\sigma$ or $\sigma^{\smile}$. Use the principle of induction for terms to arrive at the desired conclusion. $\square$

Direct products preserve all properties that are expressible by means of equations and, more generally, by means of conditional equations and open Horn formulas (see Section 2.4). In fact, equational properties hold in a direct product if and only if they hold in each factor. For the proof, consider terms

$$\sigma(v_0, \dots, v_{n-1}) \qquad \text{and} \qquad \tau(v_0, \dots, v_{n-1})$$

in the language of relation algebras. Let $\mathfrak{A} = \mathfrak{B} \times \mathfrak{C}$ be a product of algebras, and t a sequence of n elements in $\mathfrak{A}$, say with left and right coordinate sequences r and s. Lemma 11.1 implies that

$$\sigma(t) = (\sigma(r), \sigma(s)) \qquad \text{and} \qquad \tau(t) = (\tau(r), \tau(s)),$$

so the left-hand sides of these two equations are equal in $\mathfrak{A}$ if and only if the first and second coordinates on the right are equal in $\mathfrak{B}$ and in $\mathfrak{C}$ respectively. Consequently, the equation $\sigma = \tau$ is true in $\mathfrak{A}$ if and only if it is true in $\mathfrak{B}$ and true in $\mathfrak{C}$. This argument actually proves more than is claimed.

Lemma 11.2. *Suppose* $\mathfrak{A} = \mathfrak{B} \times \mathfrak{C}$.

(i) *A sequence of elements t satisfies an equation ε in $\mathfrak{A}$ if and only if the coordinate sequences r and s satisfy ε in $\mathfrak{B}$ and $\mathfrak{C}$ respectively. Consequently, t satisfies the negation of ε in $\mathfrak{A}$ if and only if at least one of the coordinate sequences r and s satisfies the negation of ε in $\mathfrak{B}$ or in $\mathfrak{C}$ respectively.*

(ii) *An equation holds in $\mathfrak{A}$ if and only if it holds in both $\mathfrak{B}$ and $\mathfrak{C}$, and it fails to hold in $\mathfrak{A}$ if and only if it fails to hold in at least one of $\mathfrak{B}$ and $\mathfrak{C}$.*

The proof that open Horn formulas are preserved under products takes a bit more work.

Lemma 11.3. *Suppose* $\mathfrak{A} = \mathfrak{B} \times \mathfrak{C}$.

(i) *If an open Horn formula Γ is satisfied by sequences r and s in $\mathfrak{B}$ and $\mathfrak{C}$ respectively, then Γ is satisfied by the product sequence t in $\mathfrak{A}$.*

(ii) *An open Horn formula holds in* $\mathfrak{A}$ *whenever it holds in* $\mathfrak{B}$ *and* $\mathfrak{C}$*.*

Proof. To prove (i), assume that sequences r and s (of the same finite length) satisfy Γ in $\mathfrak{B}$ and $\mathfrak{C}$ respectively. The formula Γ is, by definition, a disjunction of negated equations and at most one unnegated equation (see Section 2.4), so each of r and s must satisfy one of these disjuncts, by the assumption that they satisfy Γ, and by the definition of satisfaction. If r satisfies one of the negated disjuncts of Γ (in $\mathfrak{B}$), then t satisfies this same negated disjunct (in $\mathfrak{A}$), by Lemma 11.2, so t satisfies Γ. Similarly, if s satisfies one of the negated disjuncts of Γ (in $\mathfrak{C}$), then t satisfies this same negated disjunct, so again t satisfies Γ. If neither r nor s satisfies one of the negated equations of Γ, then there must be an unnegated equation in Γ that is simultaneously satisfied by both r and s, by the assumption that r and s both satisfy Γ and by the assumed form of Γ. Consequently, t satisfies this unnegated equation, by Lemma 11.2, so once again t satisfies Γ. This completes the proof of (i).

Part (ii) is an immediate consequence of (i). $\square$

It follows from Lemma 11.2(ii) that the direct product of two relation algebras is again a relation algebra, since the axioms of relation algebra are all equations. Other examples of equational properties that are preserved under the passage to a product are commutativity and symmetry. Thus, the product of two relation algebras is commutative or symmetric if and only if each of the factors is commutative or symmetric respectively. Examples of properties that are not preserved under the formation of direct products are integrality and simplicity: the product of two non-degenerate relation algebras is never integral or simple. Notice that neither of these properties can be expressed as an implication between equations.

The observations made above apply to individual elements and sequences of elements as well. For instance, an element in a direct product will possess some property that is expressed by means of an equation if and only if the left and right coordinates of the element possess the same property in the left and right factor algebras, and analogously for sequences of elements. Here is a concrete example: an element (r, s) in a product $\mathfrak{A} = \mathfrak{B} \times \mathfrak{C}$ is an ideal element if and only if r is an ideal element in $\mathfrak{B}$, and s is an ideal element in $\mathfrak{C}$. For the proof, observe that the unit in $\mathfrak{A}$ is the element $(1, 1)$. Consequently, (r, s) is an ideal element in $\mathfrak{A}$ just in case

$$(1,1)\,;(r,s)\,;(1,1)=(r,s),$$

by the definition of an ideal element. The definition of relative multiplication in $\mathfrak{A}$ implies that

$$(1,1)\,;(r,s)\,;(1,1)=(1\,;r\,;1,1\,;s\,;1).$$

Comparing the two equations, it may be concluded that (r,s) is an ideal element in $\mathfrak{A}$ if and only if $1\,;r\,;1=r$ and $1\,;s\,;1=s$, that is to say, if and only if r and s are ideal elements in $\mathfrak{B}$ and $\mathfrak{C}$ respectively. Analogous arguments lead to the conclusion that (r,s) is an equivalence element, or a right-ideal element, or a function in $\mathfrak{A}$ if and only if r and s are equivalence elements, or right-ideal elements, or functions in $\mathfrak{B}$ and $\mathfrak{C}$ respectively.

The preceding observations also apply to sets of elements, sets of sequences of elements, and so on. For example, a product of subuniverses is a subuniverse of the product, and a product of subalgebras is a subalgebra of the product. More precisely, we have the following.

Lemma 11.4. *If B_0 and C_0 are subsets of $\mathfrak{B}$ and $\mathfrak{C}$ respectively, then the set $B_0\times C_0$ is a subuniverse of the product $\mathfrak{B}\times\mathfrak{C}$ if and only if B_0 and C_0 are subuniverses of $\mathfrak{B}$ and $\mathfrak{C}$ respectively.*

Proof. The details of the arguments are rather straightforward, so it should suffice to treat an exemplary case of the proof, say the case of closure under relative multiplication. Write

$$\mathfrak{A}=\mathfrak{B}\times\mathfrak{C}\qquad\text{and}\qquad A_0=B_0\times C_0.$$

Assume first that B_0 and C_0 are subuniverses of $\mathfrak{B}$ and $\mathfrak{C}$, with the goal of showing that A_0 is closed under relative multiplication. Consider elements

$$p=(r,s)\qquad\text{and}\qquad q=(t,u)$$

in A_0. The coordinates r and t are in B_0, and s and u are in C_0, by the definition of A_0, so the relative product $r\,;t$ is in B_0, and $s\,;u$ is in C_0, by the assumption that these sets are subuniverses and are therefore closed under relative multiplication. Consequently, the pair $(r\,;t,s\,;u)$ belongs to A_0, by the definition of A_0. Since

$$p\,;q=(r,s)\,;(t,u)=(r\,;t,s\,;u),$$

by the definition of relative multiplication in $\mathfrak{A}$, it follows that the relative product $p\,;q$ belongs to A_0. Thus, A_0 is closed under relative multiplication.

To prove the reverse direction, assume A_0 is a subuniverse of $\mathfrak{A}$, with the goal of showing that B_0 and C_0 are closed under relative multiplication. The assumption on the set A_0 implies that this set contains the zero element of $\mathfrak{A}$, which is the pair $(0, 0)$; consequently, the right-coordinate of this pair must belong to C_0, by the definition of A_0. Consider now elements r and t in B_0. The pairs $(r, 0)$ and $(t, 0)$ belong to A_0, by the preceding observation and the definition of A_0, so the relative product of these pairs belongs to A_0, by the assumption that A_0 is a subuniverse and therefore closed under relative multiplication. Since

$$(r, 0)\,;(t, 0) = (r\,;t, 0\,;0),$$

by the definition of relative multiplication in $\mathfrak{A}$, it may be concluded that $r\,;t$ belongs to B_0, by the definition of A_0. Thus, B_0 is closed under relative multiplication. A similar argument shows that C_0 is closed under relative multiplication. □

Corollary 11.5. *If $\mathfrak{B}_0$ and $\mathfrak{C}_0$ are subalgebras of $\mathfrak{B}$ and $\mathfrak{C}$ respectively, then $\mathfrak{B}_0 \times \mathfrak{C}_0$ is a subalgebra of $\mathfrak{B} \times \mathfrak{C}$.*

Proof. If $\mathfrak{B}_0$ and $\mathfrak{C}_0$ are subalgebras of $\mathfrak{B}$ and $\mathfrak{C}$ respectively, then the universes B_0 and C_0 of these subalgebras are subuniverses of $\mathfrak{B}$ and $\mathfrak{C}$ respectively. Consequently, the set $B_0 \times C_0$ is a subuniverse of the product $\mathfrak{B} \times \mathfrak{C}$, by Lemma 11.4. Since the operations in

$$\mathfrak{B}_0 \times \mathfrak{C}_0 \qquad \text{and} \qquad \mathfrak{B} \times \mathfrak{C}$$

are performed coordinatewise, and since $\mathfrak{B}_0$ and $\mathfrak{C}_0$ are subalgebras of $\mathfrak{B}$ and $\mathfrak{C}$ respectively, it follows that $\mathfrak{B}_0 \times \mathfrak{C}_0$ is a subalgebra of $\mathfrak{B} \times \mathfrak{C}$. □

As another example of this type, we show that a product of homomorphisms is a homomorphism on the product. The algebras in the following lemma are all assumed to be relation algebras.

Lemma 11.6. *Suppose φ is a mapping from $\mathfrak{B}$ to $\mathfrak{B}_0$, and ψ a mapping from $\mathfrak{C}$ to $\mathfrak{C}_0$. The function ϑ defined by*

$$\vartheta((r, s)) = (\varphi(r), \psi(s))$$

is a homomorphism from $\mathfrak{B} \times \mathfrak{C}$ *to* $\mathfrak{B}_0 \times \mathfrak{C}_0$ *if and only if* φ *is a homomorphism from* $\mathfrak{B}$ *to* $\mathfrak{B}_0$, *and* ψ *a homomorphism from* $\mathfrak{C}$ *to* $\mathfrak{C}_0$. *Moreover*, ϑ *is one-to-one*, *or onto*, *or complete if and only if* φ *and* ψ *are both one-to-one*, *or both onto*, *or both complete*, *respectively*.

Proof. Again, the details of the argument are rather straightforward, so it should suffice to treat one exemplary case of the proof, say the case of relative multiplication. Write

$$\mathfrak{A} = \mathfrak{B} \times \mathfrak{C} \qquad \text{and} \qquad \mathfrak{A}_0 = \mathfrak{B}_0 \times \mathfrak{C}_0,$$

and consider elements

$$p = (r, s) \qquad \text{and} \qquad q = (t, u)$$

in $\mathfrak{A}$. The definition of ϑ implies that

$$\vartheta(p) = (\varphi(r), \psi(s)) \qquad \text{and} \qquad \vartheta(q) = (\varphi(t), \psi(u)), \tag{1}$$

so

$$\begin{aligned} \vartheta(p) ; \vartheta(q) = (\varphi(r), \psi(s)) ; (\varphi(t), \psi(u)) \\ = (\varphi(r) ; \varphi(t), \psi(s) ; \psi(u)), \end{aligned} \tag{2}$$

by (1) and the definition of relative multiplication in $\mathfrak{A}_0$. The definition of relative multiplication in $\mathfrak{A}$ implies that

$$p ; q = (r, s) ; (t, u) = (r ; t, s ; u), \tag{3}$$

so

$$\vartheta(p ; q) = \vartheta((r ; t, s ; u)) = (\varphi(r ; t), \psi(s ; u)), \tag{4}$$

by (3) and the definition of ϑ.

If φ and ψ preserve relative multiplication, then

$$\varphi(r ; t) = \varphi(r) ; \varphi(t) \qquad \text{and} \qquad \psi(s ; u) = \psi(s) ; \psi(u), \tag{5}$$

and therefore

$$\vartheta(p ; q) = \vartheta(p) ; \vartheta(q), \tag{6}$$

by (2), (4), and (5).

On the other hand, if ϑ preserves relative multiplication, then (6) is true, and therefore (5) must hold, by (2), (4), (6), and the definition of equality between ordered pairs. Conclusion: the mapping ϑ preserves relative multiplication if and only if φ and ψ both preserve relative multiplication. $\square$

One could give other examples of properties of sets that are preserved under the passage to direct products. For example, a product of ideals is an ideal in the product. Some of these examples will be explored further in the exercises.

The next lemma describes the atoms in a product in terms of the atoms in the factor algebras.

Lemma 11.7. *The atoms in the product of relation algebras $\mathfrak{B}$ and $\mathfrak{C}$ are the pairs $(r, 0)$ such that r is an atom in $\mathfrak{B}$, and the pairs $(0, s)$ such that s is an atom in $\mathfrak{C}$. The product is atomic if and only if each factor is atomic.*

Proof. Let $\mathfrak{A}$ be the product of $\mathfrak{B}$ and $\mathfrak{C}$. Every element p in $\mathfrak{A}$ has the form $p = (r, s)$ for some r in $\mathfrak{B}$ and s in $\mathfrak{C}$, by the definition of the product. The element p is an atom if and only if there is exactly one element in $\mathfrak{A}$ that is strictly below p, namely the zero element $(0, 0)$. An element $q = (t, u)$ in $\mathfrak{A}$ is below p if and only if $t \leq r$ and $u \leq s$, by the remarks at the beginning of Section 11.2. Consequently, q is strictly below p if and only if q is below p and either $t < r$ or $u < s$. Combine these observations to conclude that p is an atom in $\mathfrak{A}$ if and only if either r is an atom in $\mathfrak{B}$ and $s = 0$, or else s is an atom in $\mathfrak{C}$ and $r = 0$.

To prove the second part of the lemma, assume first that $\mathfrak{B}$ and $\mathfrak{C}$ are atomic. If $p = (r, s)$ is a non-zero element in $\mathfrak{A}$, say $r \neq 0$, then there is an atom t in $\mathfrak{B}$ that is below r, by the assumption that $\mathfrak{B}$ is atomic. The pair $q = (t, 0)$ is an atom in $\mathfrak{A}$ that is below p, by the observations of the preceding paragraph. A similar argument applies if $s \neq 0$. Thus, $\mathfrak{A}$ is atomic.

Assume now that $\mathfrak{A}$ is atomic. For every non-zero element r in $\mathfrak{B}$, there is an atom $q = (t, 0)$ that is below $p = (r, 0)$ in $\mathfrak{A}$, by the assumed atomicity of $\mathfrak{A}$. It follows from the observations of the first paragraph that t must be an atom below r in $\mathfrak{B}$. Thus, $\mathfrak{B}$ is atomic. A similar argument proves that $\mathfrak{C}$ is atomic. $\square$

Analogous arguments prove analogous assertions about the existence of suprema and infima in a product and about the completeness of the product. To formulate this result precisely, it is helpful to introduce some notation. For every subset X of a product, write

$$X_0 = \{r : (r, s) \in X \text{ for some } s\},$$
$$X_1 = \{s : (r, s) \in X \text{ for some } r\}.$$

Lemma 11.8. *If X is a subset of the product $\mathfrak{A} = \mathfrak{B} \times \mathfrak{C}$ of relation algebras, then the supremum of X exists in $\mathfrak{A}$ if and only if the suprema of the sets X_0 and X_1 exist in $\mathfrak{B}$ and $\mathfrak{C}$ respectively. If these suprema exist, then the supremum of X in $\mathfrak{A}$ is the pair consisting of the supremum of X_0 in $\mathfrak{B}$ and the supremum of X_1 in $\mathfrak{C}$. The product is complete if and only if each factor is complete.*

Proof. The equivalence

$$(r, s) \le (t, u) \qquad \text{if and only if} \qquad r \le t \text{ and } s \le u,$$

and the definitions of the sets X_0 and X_1, imply that a pair (t, u) is an upper bound of the set X in $\mathfrak{A}$ if and only if t and u are upper bounds of the sets X_0 and X_1 in $\mathfrak{B}$ and $\mathfrak{C}$ respectively. Consequently, (t, u) is the least upper bound of X in $\mathfrak{A}$ if and only if t and u are the least upper bounds of X_0 and X_1 in $\mathfrak{B}$ and $\mathfrak{C}$ respectively.

In more detail, assume (t, u) is the least upper bound of X in $\mathfrak{A}$, and consider any upper bound v of X_0 in $\mathfrak{B}$. The pair $(v, 1)$ is an upper bound of X in $\mathfrak{A}$, so the assumption on (t, u) implies that $(t, u) \le (v, 1)$ and therefore $t \le v$. Thus t is the least upper bound of X_0 in $\mathfrak{B}$. A similar argument shows that u is the least upper bound of X_1 in $\mathfrak{C}$. To establish the reverse implication, assume that t and u are the least upper bounds of X_0 and X_1 in $\mathfrak{B}$ and $\mathfrak{C}$ respectively, and consider any upper bound (v, w) of X in $\mathfrak{A}$. The elements v and w are upper bounds of X_0 and X_1 in $\mathfrak{B}$ and $\mathfrak{C}$ respectively, so the assumptions on t and v imply that $t \le v$ and $u \le w$, and therefore $(t, u) \le (v, w)$. Thus, (t, u) is the least upper bound of X.

To prove the second part of the lemma, assume first that $\mathfrak{B}$ and $\mathfrak{C}$ are complete. For an arbitrary subset X of $\mathfrak{A}$, the suprema t and u of the corresponding sets X_0 and X_1 exist in $\mathfrak{B}$ and $\mathfrak{C}$ respectively, by assumption; and the pair (t, u) is the supremum of the set X in $\mathfrak{A}$, by the observations of the first paragraph. Consequently, $\mathfrak{A}$ is complete.

Assume now that $\mathfrak{A}$ is complete, and let Y be an arbitrary subset of $\mathfrak{B}$. The set

$$X = \{(r, 0) : r \in Y\}$$

has a supremum (t, u) in $\mathfrak{A}$, by the assumption that $\mathfrak{A}$ is complete, and t must be the supremum of Y in $\mathfrak{B}$, by the observations of the first paragraph. Consequently, $\mathfrak{B}$ is complete. An analogous argument shows that $\mathfrak{C}$ is also complete. $\square$

11.3 Binary external decompositions

There are two natural mappings from a product

$$\mathfrak{A} = \mathfrak{B} \times \mathfrak{C}$$

onto the factor algebras $\mathfrak{B}$ and $\mathfrak{C}$, namely the (*left* and *right*) *projections* φ and ψ that are defined by

$$\varphi((r, s)) = r \qquad \text{and} \qquad \psi((r, s)) = s$$

for all r in $\mathfrak{B}$ and s in $\mathfrak{C}$. It is not difficult to prove that these mappings are in fact complete epimorphisms. For example, to check that the left projection φ preserves relative multiplication, observe that for pairs $p = (r, t)$ and $q = (s, u)$ in $\mathfrak{A}$, we have

$$p \,;\, q = (r \,;\, s, t \,;\, u), \qquad \varphi(p) = r, \qquad \varphi(q) = s,$$

by the definition of relative multiplication in $\mathfrak{A}$ and the definition of φ, and therefore

$$\varphi(p \,;\, q) = r \,;\, s = \varphi(p) \,;\, \varphi(q).$$

To prove that φ preserves all suprema that happen to exist, assume that $p = (r, t)$ is the supremum of a subset X of $\mathfrak{A}$, and write

$$X_0 = \{\varphi(q) : q \in X\} = \{s : (s, u) \in X \text{ for some } u\}.$$

The element r is the supremum of the set X_0, by Lemma 11.8, so

$$\varphi(p) = r = \sum X_0 = \sum\{\varphi(q) : q \in X\}.$$

The remaining arguments are left to the reader.

The congruences on a product $\mathfrak{A} = \mathfrak{B} \times \mathfrak{C}$ that are induced by the left and right projections are the relations Θ and Φ defined by

$$(r, t) \equiv (s, u) \mod \Theta \qquad \text{if and only if} \qquad r = s,$$

and

$$(r, t) \equiv (s, u) \mod \Phi \qquad \text{if and only if} \qquad t = u,$$

because

$$\varphi((r,t)) = \varphi((s,u)) \qquad \text{if and only if} \qquad r = s$$

and

$$\psi((r,t)) = \psi((s,u)) \qquad \text{if and only if} \qquad t = u,$$

by the definitions of φ and ψ. The relational composition of Θ and Φ is the universal relation $A \times A$, because for any pairs (r,t) and (s,u) in $\mathfrak{A}$,

$$(r,t) \equiv (r,u) \mod \Theta \qquad \text{and} \qquad (r,u) \equiv (s,u) \mod \Phi.$$

by the definitions of Θ and Φ. Similarly, the intersection of Θ and Φ is the identity relation id_A, because

$$(r,t) \equiv (s,u) \mod \Theta \qquad \text{and} \qquad (r,t) \equiv (s,u) \mod \Phi$$

implies that $r = s$ and $t = u$, again by the definitions of Θ and Φ. The quotients $\mathfrak{A}/\Theta$ and $\mathfrak{A}/\Phi$ are respectively isomorphic to the factors $\mathfrak{B}$ and $\mathfrak{C}$ via the functions

$$(r,s)/\Theta \longmapsto r \qquad \text{and} \qquad (r,s)/\Phi \longmapsto s$$

for each pair (r,s) in $\mathfrak{A}$, by the First Isomorphism Theorem 8.6 for congruences and the definitions of φ and ψ.

Two congruence relations on a relation algebra $\mathfrak{A}$ are said to be *orthogonal* if their composition is the universal relation $A \times A$, and their intersection is the identity relation id_A. The observations of the preceding paragraph say that the congruences associated with the two projections on a product $\mathfrak{A} = \mathfrak{B} \times \mathfrak{C}$ are orthogonal and have the additional property that the quotient of $\mathfrak{A}$ modulo each of these congruences is isomorphic to the corresponding factor algebra. It turns out that the existence of a pair of such congruences is characteristic for direct product decompositions.

Theorem 11.9. *A relation algebra $\mathfrak{A}$ is isomorphic to $\mathfrak{B} \times \mathfrak{C}$ if and only if there exists a pair of orthogonal congruences Θ and Φ on $\mathfrak{A}$ such that $\mathfrak{A}/\Theta$ and $\mathfrak{A}/\Phi$ are respectively isomorphic to $\mathfrak{B}$ and $\mathfrak{C}$.*

Proof. There are certainly congruences Θ and Φ on the product $\mathfrak{B} \times \mathfrak{C}$ with the requisite properties, by the observations preceding the theorem. If $\mathfrak{A}$ is isomorphic to $\mathfrak{B} \times \mathfrak{C}$, then the inverse images under the

isomorphism of the congruences Θ and Φ are congruences on $\mathfrak{A}$ that satisfy the conditions of the theorem.

Assume now that Θ and Φ are congruences on $\mathfrak{A}$ satisfying the conditions of the theorem, and let φ and ψ be the quotient homomorphisms from $\mathfrak{A}$ to the quotient algebras $\mathfrak{A}/\Theta$ and $\mathfrak{A}/\Phi$ respectively. Define a function ϑ from $\mathfrak{A}$ into the product $(\mathfrak{A}/\Theta) \times (\mathfrak{A}/\Phi)$ by

$$\vartheta(r) = (\varphi(r), \psi(r)) = (r/\Theta, r/\Phi)$$

for every r in $\mathfrak{A}$. We shall prove that ϑ is an isomorphism.

The homomorphism properties of φ and ψ ensure that ϑ is a homomorphism. For instance, if r and s are in $\mathfrak{A}$, then

$$\begin{aligned}\vartheta(r\,;s) = (\varphi(r\,;s), \psi(r\,;s)) &= (\varphi(r)\,;\varphi(s), \psi(r)\,;\psi(s))\\ &= (\varphi(r), \psi(r))\,;(\varphi(s), \psi(s)) = \vartheta(r)\,;\vartheta(s),\end{aligned}$$

by the definition of ϑ, the homomorphism properties of φ and ψ, and the definition of relative multiplication in a direct product.

The assumption that the intersection of Θ and Φ is the identity relation implies that ϑ is one-to-one. In more detail, if $\vartheta(r) = \vartheta(s)$, then

$$(\varphi(r), \psi(r)) = (\varphi(s), \psi(s))$$

and therefore $\varphi(r) = \varphi(s)$ and $\psi(r) = \psi(s)$. These last two equations imply that r and s are congruent modulo Θ and modulo Φ, by the definition of Θ and Φ. Since the intersection of these two congruences is the identity relation, by assumption, it follows that $r = s$.

Similarly, the assumption that the composition of Θ and Φ is the universal relation implies that ϑ is onto. For the proof, consider an arbitrary pair (p, q) of elements in the product $(\mathfrak{A}/\Theta) \times (\mathfrak{A}/\Phi)$. The quotient homomorphisms are onto mappings, so there must be elements s and t in $\mathfrak{A}$ such that $\varphi(s) = p$ and $\psi(t) = q$. The assumption that the composition of the congruences is the universal relation implies the existence of an element r in $\mathfrak{A}$ such that

$$s \equiv r \mod \Theta \qquad \text{and} \qquad r \equiv t \mod \Phi.$$

It follows from the definitions of the quotient homomorphisms that

$$\varphi(r) = \varphi(s) = p \qquad \text{and} \qquad \psi(r) = \psi(t) = q,$$

and therefore

$$\vartheta(r) = (\varphi(r), \psi(r)) = (p, q).$$

It has been shown that the function ϑ maps $\mathfrak{A}$ isomorphically to the product $(\mathfrak{A}/\Theta) \times (\mathfrak{A}/\Phi)$. The quotients $\mathfrak{A}/\Theta$ and $\mathfrak{A}/\Psi$ are assumed to be isomorphic to $\mathfrak{B}$ and $\mathfrak{C}$ respectively, so the product $(\mathfrak{A}/\Theta) \times (\mathfrak{A}/\Phi)$ is isomorphic to the product $\mathfrak{B} \times \mathfrak{C}$, by Lemma 11.6. Consequently, $\mathfrak{A}$ is isomorphic to $\mathfrak{B} \times \mathfrak{C}$, as desired. □

It is helpful to look at the preceding theorem from the perspective of ideals. Two ideals in a relation algebra $\mathfrak{A}$ are said to be *orthogonal* if their join and meet in the lattice of ideals are the improper ideal $A = (1)$ and the trivial ideal $\{0\} = (0)$ respectively. The lattice of congruences on $\mathfrak{A}$ is isomorphic to the lattice of ideals in $\mathfrak{A}$, by Theorem 8.23, so the preceding theorem can be reformulated in terms of ideals as follows.

Corollary 11.10. *A relation algebra $\mathfrak{A}$ is isomorphic to $\mathfrak{B} \times \mathfrak{C}$ if and only if there is a pair of orthogonal ideals M and N in $\mathfrak{A}$ such that $\mathfrak{A}/M$ and $\mathfrak{A}/N$ are isomorphic to $\mathfrak{B}$ and $\mathfrak{C}$ respectively.*

For any two elements r and s in a compactly generated modular lattice, if the join $r \vee s$ and meet $r \wedge s$ are both compact, then r and s must themselves be compact. (The easy proof of this assertion is left as an exercise). The lattice of ideals in a relation algebra $\mathfrak{A}$ is compactly generated and modular (and in fact, it is distributive), by Theorem 8.22. Two ideals M and N are, by definition, orthogonal if and only if their join and meet are (1) and (0) respectively. Both of these last two ideals are compact elements in the lattice of ideals, so if M and N are orthogonal, then they must be compact elements—that is to say, they must be principal ideals in $\mathfrak{A}$ (see Theorem 8.22).

Suppose now that M and N are principal ideals in $\mathfrak{A}$, say

$$M = (s) \qquad \text{and} \qquad N = (r),$$

where s and r are ideal elements in $\mathfrak{A}$. To say that M and N are orthogonal means that

$$(0) = (s) \wedge (r) = (s \cdot r) \qquad \text{and} \qquad (1) = (s) \vee (r) = (s + r),$$

by Corollary 8.18. In terms of the ideal elements themselves, these statements translate into the equations

$$s \cdot r = 0 \qquad \text{and} \qquad s + r = 1,$$

or, in different words, into the equation $s = -r$. The isomorphism of the quotients $\mathfrak{A}/M$ and $\mathfrak{A}/N$ with algebras $\mathfrak{B}$ and $\mathfrak{C}$ respectively can also be expressed in terms of ideal elements and relativizations as follows:

$$\mathfrak{A}(r) \cong \mathfrak{A}/(-r) = \mathfrak{A}/M \cong \mathfrak{B} \quad \text{and} \quad \mathfrak{A}(-r) \cong \mathfrak{A}/(r) = \mathfrak{A}/N \cong \mathfrak{C},$$

by Theorem 10.3. The following binary external version of the *Product Decomposition Theorem* has been proved.

Theorem 11.11. *A relation algebra* $\mathfrak{A}$ *is isomorphic to* $\mathfrak{B} \times \mathfrak{C}$ *if and only if there is an ideal element* r *in* $\mathfrak{A}$ *such that* $\mathfrak{B}$ *and* $\mathfrak{C}$ *are isomorphic to* $\mathfrak{A}(r)$ *and* $\mathfrak{A}(-r)$ *respectively.*

A relation algebra $\mathfrak{A}$ is said to be *directly indecomposable* if it is non-degenerate and satisfies the following condition: whenever $\mathfrak{A}$ is isomorphic to a product $\mathfrak{B} \times \mathfrak{C}$, one of factors $\mathfrak{B}$ and $\mathfrak{C}$ must be degenerate. A relativization of $\mathfrak{A}$ to an ideal element is degenerate if and only if the ideal element is 0. Consequently, the preceding theorem implies the following characterization of direct indecomposability.

Corollary 11.12. *A relation algebra is directly indecomposable if and only if it is non-degenerate and for any two ideal elements* r *and* s *in the algebra*, $r \cdot s = 0$ *and* $r + s = 1$ *implies* $r = 0$ *or* $s = 0$.

In other words, a relation algebra is directly indecomposable if and only if there is no ideal element r such that r and $-r$ are both non-zero. This immediately implies the conclusion already mentioned in Theorem 9.12 that a relation algebra is directly indecomposable if and only if it is simple.

11.4 Binary internal products

If $\mathfrak{B}$ and $\mathfrak{C}$ are set relation algebras with disjoint base sets V and W, then the product $\mathfrak{A} = \mathfrak{B} \times \mathfrak{C}$ represents itself naturally as a set relation algebra in which the base set is the union $U = V \cup W$. Before going into the details of this representation, we make several preliminary observations. First of all, the units of $\mathfrak{B}$ and $\mathfrak{C}$ are equivalence relations on the disjoint sets V and W, so the union of these two units must be an equivalence relation E on the set U, by Lemma 5.23.

Second, if a relation R on U can be written as the union of a relation S on V and a relation T on W, then S and T can be recovered from R as follows:

$$S = R \cap (V \times V) \qquad \text{and} \qquad T = R \cap (W \times W).$$

In more detail,

$$\begin{aligned} R \cap (V \times V) &= (S \cup T) \cap (V \times V) \\ &= [S \cap (V \times V)] \cup [T \cap (V \times V)] = S \cup \varnothing = S, \end{aligned}$$

by the assumption on R, the distributive law for intersection over union, the assumption that S is a relation on V and therefore a subset of $V \times V$, and the assumption that T is a relation on W and therefore disjoint from $V \times V$ (because the sets V and W are disjoint). A similar argument establishes the second equation.

Third, if each of two relations R_1 and R_2 on U can be written as the union of a relation on V and a relation on W, say

$$R_1 = S_1 \cup T_1 \qquad \text{and} \qquad R_2 = S_2 \cup T_2,$$

then

$$\begin{aligned} R_1 \cup R_2 &= (S_1 \cup S_2) \cup (T_1 \cup T_2), & \sim R_1 &= \sim S_1 \cup \sim T_1, \\ R_1 \mid R_2 &= (S_1 \mid S_2) \cup (T_1 \mid T_2), & R_1^{-1} &= S_1^{-1} \cup T_1^{-1}, \end{aligned}$$

and $id_U = id_V \cup id_W$. In the second of these last five equations, the complements of the relations S_1 and T_1 are formed with respect to the units of $\mathfrak{B}$ and $\mathfrak{C}$ respectively, while the complement of R_1 is formed with respect to union E of these two units (see above). The verification of the five equations is not difficult. As an example, here is the verification of the third one. Observe, first of all, that

$$S_1 \mid T_2 = \varnothing \qquad \text{and} \qquad T_1 \mid S_2 = \varnothing,$$

by the assumption that the base set V of the relations S_1 and S_2 is disjoint from the base set W of the relations T_1 and T_2. Use this observation and the distributive law for relational composition over union to arrive at

$$\begin{aligned} R_1 \mid R_2 &= (S_1 \cup T_1) \mid (S_2 \cup T_2) \\ &= (S_1 \mid S_2) \cup (S_1 \mid T_2) \cup (T_1 \mid S_2) \cup (T_1 \mid T_2) \\ &= (S_1 \mid S_2) \cup \varnothing \cup \varnothing \cup (T_1 \mid T_2) \\ &= (S_1 \mid S_2) \cup (T_1 \mid T_2). \end{aligned}$$

Turn now to the task of representing the product $\mathfrak{A} = \mathfrak{B} \times \mathfrak{C}$ as a set relation algebra on the union base set U. Let E be the union of the units of $\mathfrak{B}$ and $\mathfrak{C}$, as above, and define a function φ from $\mathfrak{A}$ into the full set relation algebra $\mathfrak{Re}(E)$ by

$$\varphi((S, T)) = S \cup T$$

for every pair of relations (S, T) in $\mathfrak{A}$. The second observation made above implies that φ is one-to-one. Indeed, if

$$\varphi((S_1, T_1)) = \varphi((S_2, T_2)),$$

then $S_1 \cup T_1 = S_2 \cup T_2$. Form the intersection of both sides of this equation with the relation $V \times V$ to conclude that $S_1 = S_2$, and form the intersection of both sides of the equation with the relation $W \times W$ to conclude that $T_1 = T_2$, by the second observation.

The third observation made above implies that φ is a homomorphism, and therefore a monomorphism. For example, here is the proof that φ preserves relative multiplication:

$$\begin{aligned}\varphi((S_1, T_1) \,;\, (S_2, T_2)) &= \varphi((S_1 \mid S_2, T_1 \mid T_2)) = (S_1 \mid S_2) \cup (T_1 \mid T_2) \\ &= (S_1 \cup T_1) \,|\, (S_2 \cup T_2) = \varphi((S_1, T_1)) \mid \varphi((S_2, T_2)),\end{aligned}$$

by the definition of relative multiplication in the product $\mathfrak{A}$, the definition of φ, and the third observation made above concerning relational composition. Conclusion: the function φ maps the product $\mathfrak{A}$ isomorphically to a set relation algebra that is a subalgebra of $\mathfrak{Re}(E)$.

The notion of an internal product of two relation algebras can be viewed as an extension of the preceding ideas from set relation algebras to arbitrary relation algebras.

Definition 11.13. An algebra $\mathfrak{A}$ of the same similarity type as relation algebras is called an *internal product* of two algebras $\mathfrak{B}$ and $\mathfrak{C}$ if it satisfies the following conditions.

(i) The universes of $\mathfrak{B}$ and $\mathfrak{C}$ are subsets of the universe of $\mathfrak{A}$.

(ii) Every element r in $\mathfrak{A}$ can be written in exactly one way as a sum $r = s + t$ in $\mathfrak{A}$ of elements s in $\mathfrak{B}$ and t in $\mathfrak{C}$.

(iii) For any two elements $r_1 = s_1 + t_1$ and $r_2 = s_2 + t_2$ in $\mathfrak{A}$, the following equations hold:

$$r_1 + r_2 = (s_1 + s_2) + (t_1 + t_2), \qquad -r_1 = -s_1 + -t_1,$$
$$r_1 \,;\, r_2 = (s_1 \,;\, s_2) + (t_1 \,;\, t_2), \qquad r_1\breve{} = s_1\breve{} + t_1\breve{},$$

and the identity element in $\mathfrak{A}$ is the sum in $\mathfrak{A}$ of the identity element in $\mathfrak{B}$ and the identity element in $\mathfrak{C}$. In each of the above equations, the operations on the left sides are performed in $\mathfrak{A}$, as are the middle additions on the right sides. The first and last operations on the right sides are performed in $\mathfrak{B}$ and $\mathfrak{C}$ respectively. □

The algebras $\mathfrak{B}$ and $\mathfrak{C}$ are called the (*internal*) *factors* of $\mathfrak{A}$, and the internal product is denoted by $\mathfrak{A} = \mathfrak{B} \otimes \mathfrak{C}$. If an element r in an internal product $\mathfrak{A} = \mathfrak{B} \otimes \mathfrak{C}$ is written in the form $r = s + t$ for some necessarily unique elements s in $\mathfrak{B}$ and t in $\mathfrak{C}$, then s and t are called the *components* of r (in $\mathfrak{B}$ and in $\mathfrak{C}$ respectively). The equations in condition (iii) of the preceding definition can be viewed as expressing that the operations in $\mathfrak{A}$ are performed componentwise in the factor algebras. It follows that the defined operations of multiplication and relative addition are also performed componentwise,

$$r_1 \cdot r_2 = (s_1 \cdot s_2) + (t_1 \cdot t_2), \qquad r_1 \mathbin{+\!\!\!,} r_2 = (s_1 \mathbin{+\!\!\!,} s_2) + (t_1 \mathbin{+\!\!\!,} t_2),$$

and that zero, one, and the diversity element in $\mathfrak{A}$ are the sums of the zeros, ones, and diversity elements respectively of the factor algebras $\mathfrak{B}$ and $\mathfrak{C}$.

There are a number of questions concerning internal products that need to be addressed. First, what is the relationship between an internal product and the corresponding external product? Second, to what extent is an internal product uniquely determined? Third, under what conditions does an internal product exist? We answer these questions in order.

As regards the first question, there is a canonical isomorphism from the external product of two relation algebras $\mathfrak{B}$ and $\mathfrak{C}$ to any internal product of the two algebras. Indeed, given some internal product $\mathfrak{A}$ of the two algebras, define a function φ from the external product $\mathfrak{B} \times \mathfrak{C}$ to $\mathfrak{A}$ by putting

$$\varphi((s, t)) = s + t$$

for each s in $\mathfrak{B}$ and t in $\mathfrak{C}$ (the sum being formed in $\mathfrak{A}$). The three conditions (i)–(iii) in Definition 11.13 ensure that φ is an isomorphism. First, φ is well defined and has the universe of $\mathfrak{B} \times \mathfrak{C}$ as its domain, because the universes of $\mathfrak{B}$ and $\mathfrak{C}$ are assumed to be subsets of $\mathfrak{A}$, by condition (i); consequently, one can form the sum in $\mathfrak{A}$ of any elements s from $\mathfrak{B}$ and t from $\mathfrak{C}$. Second, φ is onto because every element r in $\mathfrak{A}$

can be written as a sum $r = s + t$ for some elements s in $\mathfrak{B}$ and t in $\mathfrak{C}$, by condition (ii); therefore,

$$\varphi((s,t)) = s + t = r.$$

Third, φ is one-to-one because the representation of each element in $\mathfrak{A}$ as the sum of an element in $\mathfrak{B}$ and an element in $\mathfrak{C}$ is unique, by condition (ii); in more detail, if

$$\varphi((s,t)) = \varphi((s_1,t_1)),$$

then $s + t = s_1 + t_1$, by the definition of φ, and therefore

$$s = s_1 \qquad \text{and} \qquad t = t_1,$$

by condition (ii). Fourth, φ is a homomorphism, and therefore an isomorphism, by condition (iii). For example, here is the argument that φ preserves the operation of relative multiplication:

$$\begin{aligned}\varphi((s_1,t_1)\,;(s_2,t_2)) &= \varphi((s_1\,;s_2, t_1\,;t_2)) = (s_1\,;s_2) + (t_1\,;t_2)\\ &= (s_1 + t_1)\,;(s_2 + t_2) = \varphi((s_1,t_1))\,;\varphi((s_2,t_2)),\end{aligned}$$

by the definition of relative multiplication in the external product, the definition of φ, and the third equation in condition (iii).

As regards the second question, two internal products $\mathfrak{A}_1$ and $\mathfrak{A}_2$ of relation algebras $\mathfrak{B}$ and $\mathfrak{C}$ are always isomorphic via a mapping that is the identity function on the universe of each of the factor algebras $\mathfrak{B}$ and $\mathfrak{C}$. (These universes are subsets of each of the internal products, by condition (i), so it makes sense to say that a mapping from one internal product to another is the identity function on each of these universes.) In fact, if φ_1 and φ_2 are the canonical isomorphisms from the external product $\mathfrak{B} \times \mathfrak{C}$ to the internal products $\mathfrak{A}_1$ and $\mathfrak{A}_2$ respectively (see the preceding paragraph), then the composition $\varphi = \varphi_2 \circ \varphi_1^{-1}$ must map $\mathfrak{A}_1$ isomorphically to $\mathfrak{A}_2$ (see Figure 11.1). Moreover, each element s in $\mathfrak{B}$ is mapped to itself by φ, since

$$\varphi(s) = \varphi_2(\varphi_1^{-1}(s)) = \varphi_2((s,0)) = s + 0 = s,$$

and similarly, each element in $\mathfrak{C}$ is mapped to itself by φ. These observations justify speaking of *the* internal product of $\mathfrak{B}$ and $\mathfrak{C}$, when this product exists.

$$\begin{tikzcd}
 & \mathfrak{B} \times \mathfrak{C} \arrow[dl, "\varphi_1"'] \arrow[dr, "\varphi_2"] & \\
\mathfrak{A}_1 \arrow[rr, dashed, "\varphi"'] & & \mathfrak{A}_2
\end{tikzcd}$$

Fig. 11.1 The isomorphism between the internal products $\mathfrak{A}_1$ and $\mathfrak{A}_2$.

Turn now to the third question that was raised above: under what circumstances does the internal product $\mathfrak{A}$ of two relation algebras $\mathfrak{B}$ and $\mathfrak{C}$ exist? To motivate the answer to this question, suppose first that the internal product $\mathfrak{A} = \mathfrak{B} \otimes \mathfrak{C}$ does exist, and consider also the external product $\mathfrak{A}_0 = \mathfrak{B} \times \mathfrak{C}$. The canonical isomorphism φ from $\mathfrak{A}_0$ to $\mathfrak{A}$ maps each pair (s,t) in $\mathfrak{A}_0$ to the sum $s + t$ in $\mathfrak{A}$, so φ must map each pair $(s,0)$ to its first coordinate s, and each pair $(0,t)$ to its second coordinate t. The pairs $(1,0)$ and $(0,1)$ are ideal elements in $\mathfrak{A}_0$, and the relativizations of $\mathfrak{A}_0$ to these ideal elements are the relation algebras $\mathfrak{B}_0$ and $\mathfrak{C}_0$ with universes

$$B_0 = \{(s,0) : s \in B\} \qquad \text{and} \qquad C_0 = \{(0,t) : t \in C\}$$

respectively. It is not difficult to verify directly that $\mathfrak{A}_0$ is the internal product of the relativizations $\mathfrak{B}_0$ and $\mathfrak{C}_0$. This follows at once from Theorem 11.15 below, so we do not stop to check the details now.

The remarks made above concerning the canonical isomorphism φ show that φ maps the universes of the internal factors $\mathfrak{B}_0$ and $\mathfrak{C}_0$ (of $\mathfrak{A}_0$) to the universes of the internal factors $\mathfrak{B}$ and $\mathfrak{C}$ (of $\mathfrak{A}$) respectively. The first two internal factors are obviously disjoint, except for a common zero element that is also the zero element of $\mathfrak{A}_0$. The isomorphism properties of φ therefore imply that the second two internal factors must be disjoint, except for a common zero element that is also the zero element of $\mathfrak{A}$. Conclusion: a necessary condition for the internal product of two relation algebras to exist is that the two algebras must be disjoint except for a common zero element.

This necessary condition turns out to be sufficient as well. Indeed, suppose that relation algebras $\mathfrak{B}$ and $\mathfrak{C}$ are disjoint except for a common zero element. Form the external product $\mathfrak{A}_0 = \mathfrak{B} \times \mathfrak{C}$, and let $\mathfrak{B}_0$ and $\mathfrak{C}_0$ be the relativizations of $\mathfrak{A}_0$ that were defined above. Define functions φ_1 on $\mathfrak{B}$ and φ_2 on $\mathfrak{C}$ by

$$\varphi_1(s) = (s,0) \qquad \text{and} \qquad \varphi_2(t) = (0,t)$$

for elements s in $\mathfrak{B}$ and t in $\mathfrak{C}$. Since the operations in $\mathfrak{A}_0$ are performed coordinatewise, the mapping φ_1 is an isomorphism from $\mathfrak{B}$ to $\mathfrak{B}_0$, and the mapping φ_2 is an isomorphism from $\mathfrak{C}$ to $\mathfrak{C}_0$. Moreover, these two isomorphisms agree on the unique element that $\mathfrak{B}$ and $\mathfrak{C}$ have in common, namely zero, and otherwise they map $\mathfrak{B}$ and $\mathfrak{C}$ to disjoint subsets of $\mathfrak{A}_0$, namely B_0 and C_0 respectively. An argument very similar to the proof of the Exchange Principle (Theorem 7.15) shows that the factors $\mathfrak{B}_0$ and $\mathfrak{C}_0$ may be exchanged for $\mathfrak{B}$ and $\mathfrak{C}$ respectively, provided that the elements in $\mathfrak{A}_0$ which do not occur in $\mathfrak{B}_0$ or in $\mathfrak{C}_0$ are first replaced by new elements that do not occur in $\mathfrak{B}$ or in $\mathfrak{C}$. The result after this exchange is an algebra $\mathfrak{A}$ that is the internal product of $\mathfrak{B}$ and $\mathfrak{C}$, and that is isomorphic to $\mathfrak{A}_0$ via a function that extends both φ_1 and φ_2.

We summarize these results in the following *Existence and Uniqueness Theorem* for binary internal products.

Theorem 11.14. *The internal product of two relation algebras exists if and only if the two algebras are disjoint, except for a common zero element. If the internal product exists, then it is unique up to isomorphisms that are the identity function on the factor algebras; and the mapping* $(s,t) \longmapsto s+t$ *is an isomorphism from the external product to the internal product of the two algebras.*

The restriction in the theorem to algebras $\mathfrak{B}$ and $\mathfrak{C}$ that are disjoint except for a common zero is really insignificant. Given two arbitrary relation algebras $\mathfrak{B}$ and $\mathfrak{C}$, one can always pass first to isomorphic copies that satisfy the restriction, and then form the internal product of those isomorphic copies.

11.5 Binary internal decompositions

The close relationship between external and internal products implies that every result about external products has an analogue for internal products, and vice versa. The most important of these analogues is the binary internal version of the Product Decomposition Theorem 11.11.

Theorem 11.15. *A relation algebra* $\mathfrak{A}$ *is the internal product of relation algebras* $\mathfrak{B}$ *and* $\mathfrak{C}$ *if and only if there is an ideal element* u *in* $\mathfrak{A}$ *such that* $\mathfrak{B} = \mathfrak{A}(u)$ *and* $\mathfrak{C} = \mathfrak{A}(-u)$.

Proof. One way to prove the theorem is to derive it from Theorem 11.11, with the help of the canonical isomorphism that exists from the external to the internal product. We choose here a more direct, but longer path that avoids Theorem 11.11 and emphasizes instead the roles of conditions (i)–(iii) in Definition 11.13. These conditions will be referred to repeatedly throughout the proof.

Suppose first that an ideal element u exists in $\mathfrak{A}$ such that

$$\mathfrak{B} = \mathfrak{A}(u) \qquad \text{and} \qquad \mathfrak{C} = \mathfrak{A}(-u). \tag{1}$$

To show that $\mathfrak{A}$ is the internal product of $\mathfrak{B}$ and $\mathfrak{C}$, conditions (i)–(iii) must be verified. The universes of $\mathfrak{B}$ and $\mathfrak{C}$ are clearly subsets of $\mathfrak{A}$, by (1), so condition (i) holds.

For each element r in $\mathfrak{A}$, the products

$$s = r \cdot u \qquad \text{and} \qquad t = r \cdot -u$$

are in $\mathfrak{B}$ and in $\mathfrak{C}$ respectively, by (1) and the definition of a relativization; and

$$r = r \cdot 1 = r \cdot (u + -u) = r \cdot u + r \cdot -u = s + t,$$

by Boolean algebra; so every element in $\mathfrak{A}$ can be written as the sum of an element in $\mathfrak{B}$ and an element in $\mathfrak{C}$. If s_1 and t_1 are any other elements in $\mathfrak{B}$ and $\mathfrak{C}$ respectively such that $r = s_1 + t_1$, then

$$s = r \cdot u = (s_1 + t_1) \cdot u = s_1 \cdot u + t_1 \cdot u = s_1 + 0 = s_1,$$

and, similarly, $t = t_1$. The fourth equality holds because (1) implies that s_1 and t_1 are below u and $-u$ respectively. Thus, every element in $\mathfrak{A}$ can be written in exactly one way as the sum of an element in $\mathfrak{B}$ and an element in $\mathfrak{C}$, so condition (ii) holds.

The verifications of the equations in condition (iii) are rather similar in spirit. Here, as an example, is the verification of the third equation. Write

$$r_1 = s_1 + t_1 \qquad \text{and} \qquad r_2 = s_2 + t_2, \tag{2}$$

where s_1 and s_2 are in $\mathfrak{B}$, and t_1 and t_2 are in $\mathfrak{C}$, and observe that

$$s_1 \mathbin{;} t_2 = 0 \qquad \text{and} \qquad t_1 \mathbin{;} s_2 = 0. \tag{3}$$

In more detail,

$$s_1 ; t_2 \le u ; -u = u \cdot -u = 0,$$

by (1), the monotony law for relative multiplication, Lemmas 5.39(iv) and 5.41(ii), and Boolean algebra. The second equation in (3) is established in a similar manner. Use (2), the distributive law for relative multiplication, and (3) to arrive at

$$\begin{aligned} r_1 ; r_2 = (s_1 + t_1) ; (s_2 + t_2) &= s_1 ; s_2 + s_1 ; t_2 + t_1 ; s_2 + t_1 ; t_2 \\ &= s_1 ; s_2 + 0 + 0 + t_1 ; t_2 = s_1 ; s_2 + t_1 ; t_2 . \end{aligned}$$

The relative multiplications in this computation are all performed in $\mathfrak{A}$, but the final two can be viewed as being performed in $\mathfrak{B}$ and $\mathfrak{C}$ respectively, by (1) and the definition of relative multiplication in a relativization. This completes the proof that $\mathfrak{A}$ satisfies the conditions for being the internal product of $\mathfrak{B}$ and $\mathfrak{C}$.

To establish the reverse implication, suppose that $\mathfrak{A}$ is the internal product of $\mathfrak{B}$ and $\mathfrak{C}$. Write 1, u, and v for the units in $\mathfrak{A}$, $\mathfrak{B}$, and $\mathfrak{C}$ respectively, and observe that

$$u + v = 1 \qquad \text{and} \qquad u \cdot v = 0 \tag{4}$$

in $\mathfrak{A}$, by the remarks following Definition 11.13, so $v = -u$. In more detail, the unit in $\mathfrak{A}$ must be the sum of the units in $\mathfrak{B}$ and $\mathfrak{C}$, by the remarks following Definition 11.13 concerning the unit in $\mathfrak{A}$, so the first equation in (4) holds. Also, the elements u and v may be written as the sums of components

$$u = u + 0 \qquad \text{and} \qquad v = 0 + v,$$

so

$$u \cdot v = (u + 0) \cdot (0 + v) = u \cdot 0 + 0 \cdot v = 0 + 0,$$

by the remarks following Definition 11.13 concerning how the operation of multiplication is performed in $\mathfrak{A}$; in the preceding equations, the first two products are performed in $\mathfrak{A}$, and the third and fourth are performed in $\mathfrak{B}$ and $\mathfrak{C}$ respectively. The zero element in $\mathfrak{A}$ is the sum of the zero elements of the factors $\mathfrak{B}$ and $\mathfrak{C}$, by the remarks following Definition 11.13, so the second equation in (4) holds.

A short computation shows that u is an ideal element in $\mathfrak{A}$:

$$\begin{aligned} 1 ; u ; 1 &= (u + v) ; (u + 0) ; (u + v) \\ &= u ; u ; u + v ; 0 ; v = u + 0 = u, \end{aligned}$$

where the relative multiplications in the first two terms are performed in $\mathfrak{A}$ and the relative multiplications in the third term are performed in $\mathfrak{B}$ and $\mathfrak{C}$ respectively. The first equality uses the observations of the preceding paragraph, the second uses the third equation in condition (iii), and the third uses the fact that u is the unit of $\mathfrak{B}$, so $u ; u ; u = u$ (in $\mathfrak{B}$), by Lemma 4.5(iv).

Turn now to the task of establishing (1), and focus on the first equation in (1). Consider an arbitrary element r. If r belongs to $\mathfrak{B}$, then r is below the unit u of $\mathfrak{B}$, and r also belongs to $\mathfrak{A}$, by condition (i), so r belongs to $\mathfrak{A}(u)$, by the definition of this relativization. Assume now that r belongs to $\mathfrak{A}(u)$. Certainly, r is in $\mathfrak{A}$, by the definition of a relativization, so there must be elements s and t in $\mathfrak{B}$ and $\mathfrak{C}$ respectively such that $r = s + t$, by condition (ii). The assumption on r also implies that r is below u, so we have

$$r = r \cdot u = (s + t) \cdot (u + 0) = s \cdot u + t \cdot 0 = s.$$

The third equality uses condition (iii) as it applies to multiplication, and the fourth equality uses the fact that s is in $\mathfrak{B}$ and therefore below the unit u of $\mathfrak{B}$. This computation shows that r coincides with an element in $\mathfrak{B}$. Conclusion: the algebras $\mathfrak{B}$ and $\mathfrak{A}(u)$ have the same universes.

Consider next the operations of the two algebras. We prove, as an example, that relative multiplication in $\mathfrak{B}$ coincides with relative multiplication in $\mathfrak{A}(u)$. Assume r_1 and r_2 are elements in $\mathfrak{B}$. The unique way of writing these two elements as sums of elements in $\mathfrak{B}$ and in $\mathfrak{C}$ is obviously just

$$r_1 = r_1 + 0 \qquad \text{and} \qquad r_2 = r_2 + 0.$$

Apply the third equation in condition (iii) to obtain

$$r_1 ; r_2 = r_1 ; r_2 + 0 ; 0 = r_1 ; r_2 + 0 = r_1 ; r_2,$$

where the first relative multiplication is performed in $\mathfrak{A}$, the second in $\mathfrak{B}$, the third in $\mathfrak{C}$, and the fourth and fifth in $\mathfrak{B}$. Since the operation of relative multiplication in $\mathfrak{A}(u)$ is the restriction of the operation of relative multiplication in $\mathfrak{A}$, the preceding computation shows that the relative product of r_1 and r_2 in $\mathfrak{A}(u)$ coincides with the relative product of r_1 and r_2 in $\mathfrak{B}$. In other words, $\mathfrak{B}$ and $\mathfrak{A}(u)$ have the same operation of relative multiplication. Analogous arguments show that

the remaining operations and distinguished constants of the two algebras coincide. Thus, the first equation in (1) holds. Similar arguments establish the second equation in (1). □

In one respect, external products have a distinct advantage over internal products: the definition of an external product is quite general and straightforward, and one does not have to be concerned about problems of existence and uniqueness. On the other hand, internal products have a number of advantages over external products. One advantage is notational: each element in the internal product can be written in a unique way as a sum of elements in the two factor algebras, and every element in each factor really does belong to the internal product; with external products one always has to speak of ordered pairs of elements, and the elements of the factor algebras do not, in general, belong to the external product. A similar remark applies to the operations: the operations of the factor algebras really are restrictions (or, in the case of complementation, relativized restrictions) of the corresponding operations of the internal product, but they are not restrictions of the corresponding operations of the external product.

The notational simplicity of internal products over external products carries with it another advantage: results about products often have an easier and more intuitive formulation in their internal version than in their external version. For example, in Lemma 11.7 one must describe the atoms in the external product as certain copies of the atoms in the factor algebras, because the elements in the factor algebras do not belong to the external product. In the internal version of this lemma, one can simply describe the atoms in the internal product as the atoms of the factor algebras.

Yet another advantage of internal products is that they often make it possible to avoid the introduction of isomorphisms and isomorphic copies, whereas with external products one must almost always speak of isomorphisms and isomorphic copies. For example, in the external version of the Product Decomposition Theorem 11.11, one has to say (and prove) that the factor algebras $\mathfrak{B}$ and $\mathfrak{C}$ are isomorphic to relativizations of the external product $\mathfrak{A}$. There is no way to avoid the introduction of isomorphisms in this theorem; it is just not true that $\mathfrak{B}$ and $\mathfrak{C}$ are relativizations of $\mathfrak{A}$. On the other hand, in the internal version of this theorem (Theorem 11.15), the factor algebras $\mathfrak{B}$ and $\mathfrak{C}$ really are relativizations of the internal product $\mathfrak{A}$.

To summarize, there is an initial price that must be paid for using internal products: the definition is less straightforward than the definition of an external product, and certain questions regarding existence and uniqueness must be addressed. These initial costs are counterbalanced by some long-term advantages: many discussions about products—and in particular, the formulations and proofs of many theorems—become notationally and terminologically simpler and more direct when one uses internal products.

11.6 General external products

Almost everything that has been said so far about products of two relation algebras can be generalized to products of arbitrary systems of relation algebras. The development is parallel to the one for binary products, so our presentation will be briefer.

By the *direct product* of a system $(\mathfrak{A}_i : i \in I)$ of relation algebras, we understand the algebra

$$\mathfrak{A} = \prod_{i\in I} \mathfrak{A}_i,$$

of the same similarity type as relation algebras, that is defined as follows. The universe of $\mathfrak{A}$ is the set of functions r with domain I such that $r(i)$—or r_i, as we shall often write—is an element of $\mathfrak{A}_i$ for each index i. The operations of $\mathfrak{A}$ are performed coordinatewise. This means that the sum and relative product of functions r and s in $\mathfrak{A}$ are the functions $r + s$ and $r \mathbin{;} s$ on I that are defined by

$$(r + s)_i = r_i + s_i \qquad \text{and} \qquad (r \mathbin{;} s)_i = r_i \mathbin{;} s_i$$

for each i. The complement and converse of a function r in $\mathfrak{A}$ are the functions $-r$ and $r^{\smile}$ on I that are defined by

$$(-r)_i = -r_i \qquad \text{and} \qquad (r^{\smile})_i = r_i^{\smile}$$

for each i. The operations on the left sides of these equations are the ones being defined in $\mathfrak{A}$, while the ones on the right are the corresponding operations in $\mathfrak{A}_i$. The identity element in $\mathfrak{A}$ is the function 1' on I that is defined by $1'_i = 1'$ for each i, where the element 1' on the right side of this equation is the identity element in $\mathfrak{A}_i$. The algebras $\mathfrak{A}_i$ are called the *direct factors* of the product $\mathfrak{A}$.

As in the case of binary products, we may also refer to $\mathfrak{A}$ as the *Cartesian product*, or the *external product*, of the system $(\mathfrak{A}_i : i \in I)$, and we may refer to the algebras $\mathfrak{A}_i$ as the *external factors* of $\mathfrak{A}$. When no confusion can arise, we may simplify the terminology by speaking of the *product* of the system, and the *factors* of the product.

Two observations are in order. First, the index set I is allowed to be empty. In this case there is just one function with domain I, namely the empty function, so the product of the system is the degenerate (one-element) algebra. Second, when all the factors $\mathfrak{A}_i$ are equal to the same algebra $\mathfrak{B}$, the product $\prod_{i\in I} \mathfrak{A}_i$ is called a *power* of $\mathfrak{B}$, or more precisely, the Ith *power* of $\mathfrak{B}$, and is usually written as $\mathfrak{B}^I$.

11.7 Properties preserved under general products

The defined operations, relations, and distinguished constants in the product $\mathfrak{A} = \prod_{i\in I} \mathfrak{A}_i$ are also determined coordinatewise. For example, the operations of multiplication and relative addition, when applied to functions r and s in $\mathfrak{A}$, yield the functions $r \cdot s$ and $r \mathbin{\underset{,}{+}} s$ in $\mathfrak{A}$ that are determined by the formulas

$$(r \cdot s)_i = r_i \cdot s_i \qquad \text{and} \qquad (r \mathbin{\underset{,}{+}} s)_i = r_i \mathbin{\underset{,}{+}} s_i$$

for each i. The distinguished elements zero, one, and the diversity element in $\mathfrak{A}$ are the functions 0, 1, and 1’ that are determined by

$$0_i = 0, \qquad 1_i = 1, \qquad 0'_i = 0',$$

for each i, where the elements on the right sides of these equations are the distinguished constants zero, one, and the diversity element in $\mathfrak{A}_i$. The ordering relation in $\mathfrak{A}$ is determined by the equivalence

$$r \leq s \qquad \text{if and only if} \qquad r_i \leq s_i$$

for each i.

More generally, any operation on the universe of $\mathfrak{A}$ that can be defined by means of a term in the language of relation algebras is performed coordinatewise. To state this result precisely, it is helpful to introduce some terminology. If

$$t = (r^{(0)}, \ldots, r^{(n-1)})$$

is a sequence of elements in $\mathfrak{A}$, then for each index i in I, the sequence

$$t^{(i)} = (r_i^{(0)}, \ldots, r_i^{(n-1)})$$

in the factor algebra $\mathfrak{A}_i$ is called the ith *coordinate sequence* of t, and t is called the *product sequence* of $t^{(0)}, \ldots, t^{(n-1)}$.

Lemma 11.16. *Let $\gamma(v_0, \ldots, v_{n-1})$ be a term in the language of relation algebras, and t a sequence of n elements in a direct product*

$$\mathfrak{A} = \textstyle\prod_{i \in I} \mathfrak{A}_i .$$

If $t^{(i)}$ is the ith *coordinate sequence of t, then*

$$\gamma^{\mathfrak{A}}(t) = (\gamma^{\mathfrak{A}_i}(t^{(i)}) : i \in I).$$

Proof. The proof is a straightforward generalization of the corresponding proof for binary products (see Lemma 11.1), but the details have a superficially different and more complicated appearance. Assume that

$$t = (r^{(0)}, \ldots, r^{(n-1)}), \tag{1}$$

write $t^{(i)}$ for the ith coordinate sequence of t, and observe that

$$t_j^{(i)} = r_i^{(j)} \tag{2}$$

for each index i in I and each $j = 0, \ldots, n-1$.

The proof of the lemma proceeds by induction on terms. There are two base cases to consider. If γ is a variable v_j, then

$$\gamma^{\mathfrak{A}}(t) = r^{(j)} = (r_i^{(j)} : i \in I) = (t_j^{(i)} : i \in I) = (\gamma^{\mathfrak{A}_i}(t^{(i)}) : i \in I),$$

by (1), the definition of the value of a term on a sequence of elements in an algebra (see Section 2.4), and (2). A similar argument applies if γ is the distinguished constant 1’.

Assume now as the induction hypothesis that σ and τ are terms whose values on t are determined by

$$\sigma^{\mathfrak{A}}(t) = (\sigma^{\mathfrak{A}_i}(t^{(i)}) : i \in I) \quad \text{and} \quad \tau^{\mathfrak{A}}(t) = (\tau^{\mathfrak{A}_i}(t^{(i)}) : i \in I). \tag{3}$$

There are four cases to consider. If γ is the term $\sigma \,;\, \tau$, then

$$\begin{aligned}
\gamma^{\mathfrak{A}}(t) &= (\sigma \,;\, \tau)^{\mathfrak{A}}(t) \\
&= \sigma^{\mathfrak{A}}(t) \,;\, \tau^{\mathfrak{A}}(t) \\
&= (\sigma^{\mathfrak{A}_i}(t^{(i)}) : i \in I) \,;\, (\tau^{\mathfrak{A}_i}(t^{(i)}) : i \in I) \\
&= (\sigma^{\mathfrak{A}_i}(t^{(i)}) \,;\, \tau^{\mathfrak{A}_i}(t^{(i)}) : i \in I) \\
&= ((\sigma \,;\, \tau)^{\mathfrak{A}_i}(t^{(i)}) : i \in I) \\
&= (\gamma^{\mathfrak{A}_i}(t^{(i)}) : i \in I).
\end{aligned}$$

The first and last equalities use the assumption on γ, and the second and fifth use the definition of the value of a term on a sequence of elements in an algebra. The third equality uses the induction hypotheses in (3), and the fourth uses the fact that the operation $;$ in $\mathfrak{A}$ is defined coordinatewise in terms of the corresponding operations in the factor algebras $\mathfrak{A}_i$. Thus, the conclusion of the lemma holds in this case. A similar argument applies if γ is one of the terms $\sigma + \tau$, or $-\sigma$ or $\sigma^{\smile}$. Use the principle of induction for terms to arrive at the desired conclusion. □

As in the binary case, direct products preserve all properties that are expressible by means of equations, and more generally by means of conditional equations and open Horn formulas. We begin with the generalization of Lemma 11.2

Lemma 11.17. *Suppose $\mathfrak{A}$ is the product of a non-empty system of algebras, say $\mathfrak{A} = \prod_i \mathfrak{A}_i$.*

(i) *A sequence of elements t satisfies an equation ε in $\mathfrak{A}$ if and only if, for each index i, the* ith *coordinate sequence of t satisfies ε in $\mathfrak{A}_i$. Consequently, t satisfies the negation of ε in $\mathfrak{A}$ if and only if, for some index i, the* ith *coordinate sequence of t satisfies the negation of ε in $\mathfrak{A}_i$.*

(ii) *An equation holds in $\mathfrak{A}$ if and only if it holds in each factor $\mathfrak{A}_i$, and it fails to hold in $\mathfrak{A}$ if and only if it fails to hold in at least one of the factors.*

Proof. The proof of (i) is a straightforward generalization of the corresponding result for binary products (see Lemma 11.2), but again the details have a superficially different appearance. Consider an equation

$$\sigma(v_0, \ldots, v_{n-1}) = \tau(v_0, \ldots, v_{n-1})$$

in the language of relation algebras, and let t be a sequence of n elements in the product $\mathfrak{A}$. Lemma 11.16 implies that

$$\sigma^{\mathfrak{A}}(t) = (\sigma^{\mathfrak{A}_i}(t^{(i)}) : i \in I) \qquad \text{and} \qquad \tau^{\mathfrak{A}}(t) = (\tau^{\mathfrak{A}_i}(t^{(i)}) : i \in I),$$

so

$$\sigma^{\mathfrak{A}}(t) = \tau^{\mathfrak{A}}(t) \qquad \text{if and only if} \qquad \sigma^{\mathfrak{A}_i}(t^{(i)}) = \tau^{\mathfrak{A}_i}(t^{(i)})$$

for each index i. This proves the first assertion in (i). The second assertion in (i) is an immediate consequence of the first, and (ii) follows at once from (i). □

To avoid later confusion, it is worthwhile looking for a moment at the case when the system of algebras is empty. In this case, the direct product of the system is a one-element algebra (see the final paragraph of Section 11.6), so every equation is automatically true in the product and therefore the negation of every equation is false. It follows that every conditional equation is true in the product, and every open Horn formula that is a disjunction of negated equations is false.

Here is the generalization of Lemma 11.3. The proof is left as an exercise.

Lemma 11.18. *Suppose $\mathfrak{A}$ is the product of a non-empty system of algebras, say $\mathfrak{A} = \prod_i \mathfrak{A}_i$.*

(i) *If an open Horn formula Γ is satisfied by a sequence $t^{(i)}$ in $\mathfrak{A}_i$ for each index i, then Γ is satisfied by the product sequence in $\mathfrak{A}$.*
(ii) *An open Horn formula holds in $\mathfrak{A}$ whenever it holds in each factor $\mathfrak{A}_i$.*

For the special case of Lemma 11.18 when the open Horn formulas are conditional equations, the proviso that the system of algebras be non-empty is unnecessary. Indeed, as was pointed out before the lemma, conditional equations are always true in the degenerate algebra that is the product of an empty system of algebras.

Lemma 11.17(ii) and the remark following it imply that the product of a system of relation algebras is again a relation algebra. More generally, any property of relation algebras that is expressible by means of equations is preserved under products. For example, a product of relation algebras is commutative or symmetric if and only if each factor is commutative or symmetric respectively. Also, the observations made in Section 11.2 about the preservation of properties concerning

individual elements or sequences of elements in binary products apply in the case of general products as well. Thus, an element r in a direct product is an ideal element if and only if each coordinate r_i is an ideal element in the corresponding factor algebra, and the same is true for the notions of an equivalence element, a right-ideal element, a subidentity element, and a function.

The same remarks apply to sets of elements, sets of sequences of elements, and so on. As examples, here are the extensions to general products of some of the results stated in the second half of Section 11.2. The proofs are easy variants of the earlier proofs, and are left as exercises.

Lemma 11.19. *If B_i is a subset of $\mathfrak{A}_i$ for each i in some index set, then the product set $\prod_i B_i$ is a subuniverse of the product algebra $\prod_i \mathfrak{A}_i$ if and only if B_i is a subuniverse of $\mathfrak{A}_i$ for each i.*

The extension of Corollary 11.5 says that a general product of subalgebras is a subalgebra of the general product.

Corollary 11.20. *If $\mathfrak{B}_i$ is a subalgebra of $\mathfrak{A}_i$ for each i in some index set, then the product $\prod_i \mathfrak{B}_i$ is a subalgebra of the product $\prod_i \mathfrak{A}_i$.*

The extension of Lemma 11.6 says that a general product of homomorphisms is a homomorphism of the product. We shall revisit this lemma again later, in the context of general internal products.

Lemma 11.21. *Suppose φ_i is a mapping from $\mathfrak{A}_i$ to $\mathfrak{B}_i$ for each i in some index set I. The function φ defined by*

$$\varphi(r) = (\varphi_i(r_i) : i \in I)$$

for r in $\prod_i \mathfrak{A}_i$ is a homomorphism from $\prod_i \mathfrak{A}_i$ to $\prod_i \mathfrak{B}_i$ if and only if φ_i is a homomorphism for each i. Moreover, φ is one-to-one, or onto, or complete if and only if the mappings φ_i are all one-to-one, or all onto, or all complete respectively.

The preceding lemma justifies calling the mapping φ the *product homomorphism* of the system $(\varphi_i : i \in I)$, and calling the mappings φ_i the *factors* of φ.

The next lemma is the extension of Lemma 11.7 to general products.

Lemma 11.22. *The atoms in a product $\mathfrak{A} = \prod_i \mathfrak{A}_i$ of relation algebras are the elements r in $\mathfrak{A}$ such that r_i is an atom in $\mathfrak{A}_i$ for exactly one index i, and $r_j = 0$ for all indices $j \neq i$. The product algebra is atomic if and only if each factor algebra is atomic.*

To state the extension of Lemma 11.8 to general products, it is helpful to introduce some notation: for every subset X of a general product, write

$$X_i = \{r_i : r \in X\}.$$

Lemma 11.23. *If X is a subset of a product $\mathfrak{A} = \prod_i \mathfrak{A}_i$ of relation algebras, then the supremum of X exists in $\mathfrak{A}$ if and only if the supremum of the set X_i exists in $\mathfrak{A}_i$ for each i. If these suprema exist, then the supremum of X is the function r in $\mathfrak{A}$ such that r_i is the supremum of X_i in $\mathfrak{A}_i$ for each i. The product algebra is complete if and only if each factor algebra is complete.*

11.8 General external decompositions

A representation of a relation algebra $\mathfrak{A}$ as an isomorphic copy of the direct product of a system of relation algebras is called an (*external*) *direct decomposition* of $\mathfrak{A}$. The purpose of this section is to characterize when such a decomposition is possible.

For each index i, there is a natural mapping from a product

$$\mathfrak{A} = \prod_{j \in I} \mathfrak{A}_j$$

onto the factor algebra $\mathfrak{A}_i$, namely the ith *projection* φ_i that is defined by $\varphi_i(r) = r_i$ for each r in $\mathfrak{A}$. This mapping is in fact a complete epimorphism from $\mathfrak{A}$ to $\mathfrak{A}_i$. The proof is but a variant of the proof of the analogous result for binary products. As an example, here is the verification that φ_i preserves relative multiplication. For elements r and s in $\mathfrak{A}$, if $t = r \,;\, s$, then $t_i = r_i \,;\, s_i$ for each i, by the definition of relative multiplication in $\mathfrak{A}$, and therefore

$$\varphi_i(r \,;\, s) = \varphi_i(t) = t_i = r_i \,;\, s_i = \varphi_i(r) \,;\, \varphi_i(s).$$

The congruence on the product $\mathfrak{A}$ that is induced by the projection φ_i is the relation Θ_i determined by

$$r \equiv s \mod \Theta_i \qquad \text{if and only if} \qquad r_i = s_i$$

for all r and s in $\mathfrak{A}$, since

$$\varphi_i(r) = \varphi_i(s) \qquad \text{if and only if} \qquad r_i = s_i,$$

by the definition of φ_i. The system $(\Theta_i : i \in I)$ of these congruences has a number of important properties. The first property is that the intersection $\bigcap_i \Theta_i$ of the system of congruences is the identity relation id_A on $\mathfrak{A}$. Indeed, if $r \equiv s \mod \Theta_i$ for each i, then $r_i = s_i$ for each i, by the definition of Θ_i, and therefore $r = s$. The second property is that if $s^{(i)}$ is an element in the product $\mathfrak{A}$ for each index i in I (so that $(s^{(i)} : i \in I)$ is a system of elements in $\mathfrak{A}$), then there is an element r in $\mathfrak{A}$ such that

$$r \equiv s^{(i)} \mod \Theta_i$$

for each i. Just take r to be the element in $\mathfrak{A}$ defined by $r_i = s_i^{(i)}$ for each i (where $s_i^{(i)}$ is the value of the function $s^{(i)}$ on the index i), and apply the definition of Θ_i. The third property is that the quotient $\mathfrak{A}/\Theta_i$ is isomorphic to the factor algebra $\mathfrak{A}_i$ via the function $r/\Theta_i \longmapsto r_i$, by the First Isomorphism Theorem 8.6 for congruences.

An arbitrary system $(\Theta_i : i \in I)$ of congruences on a relation algebra $\mathfrak{A}$ is said to be *orthogonal* if it possesses the first two properties in the preceding paragraph. The observations of that paragraph can be summarized by saying that the congruences associated with the projections on a product $\mathfrak{A} = \prod_i \mathfrak{A}_i$ form an orthogonal system and have the additional property that for each i, the quotient of $\mathfrak{A}$ modulo the congruence Θ_i is isomorphic to the factor $\mathfrak{A}_i$. The existence of a system of congruences with these properties is characteristic for direct product decompositions.

Theorem 11.24. *A relation algebra $\mathfrak{A}$ is isomorphic to a product $\prod_{i \in I} \mathfrak{A}_i$ if and only if there is an orthogonal system $(\Theta_i : i \in I)$ of congruences on $\mathfrak{A}$ such that $\mathfrak{A}/\Theta_i$ is isomorphic to $\mathfrak{A}_i$ for each i.*

Proof. The proof is similar to the proof of Theorem 11.9. There is certainly a system $(\Theta_i : i \in I)$ of congruences on the product $\prod_i \mathfrak{A}_i$ with the requisite properties, by the observations preceding the theorem. If the algebra $\mathfrak{A}$ is isomorphic to this product, then the inverse images of the congruences Θ_i under the isomorphism form a system of congruences on $\mathfrak{A}$ that satisfies the conditions of the theorem.

Assume now that $(\Theta_i : i \in I)$ is a system of congruences on $\mathfrak{A}$ satisfying the conditions of the theorem, and for each i, let φ_i be the quotient homomorphism from $\mathfrak{A}$ to the quotient algebra $\mathfrak{A}/\Theta_i$. Define a function φ from $\mathfrak{A}$ into the product

$$\mathfrak{B} = \prod_i \mathfrak{A}/\Theta_i \tag{1}$$

by

$$\varphi(r) = (\varphi_i(r) : r \in I) = (r/\Theta_i : i \in I) \tag{2}$$

for every r in $\mathfrak{A}$. We shall prove that φ is an isomorphism.

The homomorphism properties of the quotient homomorphisms ensure that φ is a homomorphism. For example, if r and s are elements in $\mathfrak{A}$, then

$$\begin{aligned}\varphi(r\,;s) = (\varphi_i(r\,;s) : i \in I) &= (\varphi_i(r)\,;\varphi_i(s) : i \in I)\\ &= (\varphi_i(r) : i \in I)\,;(\varphi_i(s) : i \in I) = \varphi(r)\,;\varphi(s),\end{aligned}$$

by the definition of φ, the homomorphism properties of the mappings φ_i, and the definition of relative multiplication in $\mathfrak{B}$.

The assumption that the intersection of the given system of congruences is the identity relation id_A ensures that φ is one-to-one. In more detail, if $\varphi(r) = \varphi(s)$, then

$$r/\Theta_i = s/\Theta_i$$

for every i, by (2), so the pair (r, s) belongs to every congruence Θ_i in the system. Consequently, this pair belongs to the intersection of the system, and therefore $r = s$, by the assumption that the intersection is id_A.

To check that φ is onto, consider an arbitrary element s in the product $\mathfrak{B}$. By (1), s has the form

$$s = (s^{(i)}/\Theta_i : i \in I),$$

where $s^{(i)}$ is an element in $\mathfrak{A}$ for each i. The assumed orthogonality of the system of congruences guarantees the existence of an element r in $\mathfrak{A}$ with the property that $r \equiv s^{(i)} \mod \Theta_i$, and therefore

$$\varphi_i(r) = \varphi_i(s^{(i)}) = s^{(i)}/\Theta_i,$$

for each i. It follows that

$$\varphi(r) = (\varphi_i(r) : i \in I) = (s^{(i)}/\Theta_i : i \in I) = s.$$

Conclusion: φ maps $\mathfrak{A}$ isomorphically to $\mathfrak{B}$.

The quotient $\mathfrak{A}/\Theta_i$ is assumed to be isomorphic to $\mathfrak{A}_i$ for each i, so $\mathfrak{B}$ must be isomorphic to the product $\prod_i \mathfrak{A}_i$, by (1) and Lemma 11.21. Consequently, $\mathfrak{A}$ is also isomorphic to $\prod_i \mathfrak{A}_i$. $\square$

Before proceeding further, we prove a lemma that will be needed shortly. It says that each congruence in a system of orthogonal congruences is orthogonal to the intersection of the remaining congruences.

Lemma 11.25. *If $(\Theta_i : i \in I)$ is an orthogonal system of congruences on a relation algebra, then for each index i, the two congruences Θ_i and $\bigcap_{j \neq i} \Theta_j$ are orthogonal.*

Proof. Let $\mathfrak{A}$ be the relation algebra under consideration, and write

$$\Phi = \bigcap_{j \neq i} \Theta_j .$$

It is to be shown that

$$\Theta_i \cap \Phi = id_A \qquad \text{and} \qquad \Theta_i \,|\, \Phi = A \times A. \tag{1}$$

The intersection of Θ_i and Φ coincides with the intersection of the entire system of congruences, by the definition of Φ, and the intersection of the entire system is id_A, by the assumption that the system is orthogonal, so the first equation in (1) holds.

In order to establish the second equation in (1), consider any two elements t and u in $\mathfrak{A}$. Write

$$s^{(i)} = t, \qquad \text{and} \qquad s^{(j)} = u \tag{2}$$

for $j \neq i$. The assumed orthogonality of the given system of congruences implies the existence of an element r in $\mathfrak{A}$ such that

$$r \equiv s^{(j)} \mod \Theta_j$$

for each index j. Take first $j = i$ and then $j \neq i$, and use (2), to obtain

$$t \equiv s^{(i)} \equiv r \mod \Theta_i \qquad \text{and} \qquad u \equiv s^{(j)} \equiv r \mod \Theta_j$$

respectively. The equivalence on the left implies that the pair (t, r) is in the congruence Θ_i. The equivalence on the right implies that the pair (r, u) is in each of the congruences Θ_j for $j \neq i$, and is therefore in their intersection Φ. Conclusion: the pair (t, u) is in the composition of Θ_i and Φ, by the definition of relational composition, so the second equation in (1) holds. □

We now look at Theorem 11.24 from the perspective of ideals. A system $(M_i : i \in I)$ of ideals in a relation algebra $\mathfrak{A}$ is said to be

orthogonal if the intersection of the system is the trivial ideal (0) and if, for each system $(s^{(i)} : i \in I)$ of elements in $\mathfrak{A}$, there is an element r in $\mathfrak{A}$ such that $r/M_i = s^{(i)}/M_i$ for every index i. The first condition is equivalent to the corresponding condition for systems of congruences, because the lattice of ideals in $\mathfrak{A}$ is canonically isomorphic to the lattice of congruences on $\mathfrak{A}$, by Theorem 8.23. The second condition is identical to the corresponding condition for systems of congruences, because the quotient of an element modulo an ideal is equal to the quotient of the element modulo the corresponding congruence. Consequently, a system of ideals is orthogonal if and only if the corresponding system of congruences is orthogonal. This permits us to reformulate Theorem 11.24 in terms of ideals.

Corollary 11.26. *A relation algebra $\mathfrak{A}$ is isomorphic to a product $\prod_{i\in I}\mathfrak{A}_i$ if and only if there is an orthogonal system $(M_i : i \in I)$ of ideals in $\mathfrak{A}$ such that $\mathfrak{A}/M_i$ is isomorphic to $\mathfrak{A}_i$ for each i.*

Suppose $(M_i : i \in I)$ is an orthogonal system of ideals in $\mathfrak{A}$. For each index i, the ideal M_i must be orthogonal to the intersection

$$N = \bigcap_{j\neq i} M_j$$

of the remaining ideals in the system, by Lemma 11.25 and the isomorphism between the lattice of ideals and the lattice of congruences (Theorem 8.23). Consequently, M_i and N must be principal ideals, by the observations following Corollary 11.10. In particular, each of the ideals in an orthogonal system of ideals must be principal.

Motivated by the conclusion of the previous paragraph, we now prove a lemma that gives two closely related characterizations of when a system of principal ideals is orthogonal. In the formulation and proof of the lemma, we simplify the notation somewhat by using the subscript notation s_i, t_i, etc. to refer to elements in $\mathfrak{A}$ instead of to elements in $\mathfrak{A}_i$. (In the lemma, there are no algebras $\mathfrak{A}_i$.)

Lemma 11.27. *The following conditions on a system $(v_i : i \in I)$ of ideal elements in a relation algebra $\mathfrak{A}$ are equivalent.*

(i) *The system $((v_i) : i \in I)$ of principal ideals is orthogonal.*
(ii) *The system $(v_i : i \in I)$ satisfies the following conditions.*

  (a) $\prod_i v_i = 0$.
  (b) $v_i + v_j = 1$ *for* $i \neq j$.

(c) *Whenever* $(r_i : i \in I)$ *is a system of elements in* $\mathfrak{A}$ *with* $r_i \geq v_i$ *for each* i, *the product* $\prod_i r_i$ *exists in* $\mathfrak{A}$.

(iii) *The system* $(u_i : i \in I)$ *of complementary ideal elements* $u_i = -v_i$ *satisfies the following conditions.*

(a) $\sum_i u_i = 1$.
(b) $u_i \cdot u_j = 0$ *for* $i \neq j$.
(c) *Whenever* $(r_i : i \in I)$ *is a system of elements in* $\mathfrak{A}$ *with* $r_i \leq u_i$ *for each* i, *the sum* $\sum_i r_i$ *exists in* $\mathfrak{A}$.

Proof. Each of the conditions (a)–(c) in (ii) is equivalent to the corresponding condition in (iii). For parts (a) and (b), this is obvious, by Boolean algebra. To establish the equivalence for part (c), assume condition (ii)(c) holds and consider an arbitrary system $(r_i : i \in I)$ of elements in $\mathfrak{A}$ with $r_i \leq u_i$ for each i. Write $s_i = -r_i$ for each i, and observe that $s_i \geq v_i$, by Boolean algebra and the definition of the elements u_i. Apply (ii)(c) to the system $(s_i : i \in I)$ to obtain the existence of the product $s = \prod_i s_i$ in $\mathfrak{A}$. The complement of s must also exist in $\mathfrak{A}$, and this complement is just the sum $\sum_i r_i$, by Boolean algebra. Thus, condition (iii)(c) holds. The reverse implication, from (iii)(c) to (ii)(c), is established by a completely analogous argument.

To establish the implication from (i) to (iii), assume the hypothesis of (i). The intersection of the system of ideals in (i) must then be the trivial ideal, by the definition of orthogonality, so condition (ii)(a) holds, by Lemma 8.19(ii). Hence, condition (iii)(a) also holds, by the equivalence of (ii)(a) and (iii)(a) established in the previous paragraph. For each index i, the ideal (v_i) is orthogonal to the intersection $\bigcap_{j \neq i}(v_j)$ of the remaining ideals, by the remarks preceding the lemma, so the join of the ideal (v_i) with this intersection must be the improper ideal (1), by the definition of orthogonality for pairs of ideals (see the remarks preceding Corollary 11.10). It follows that the join of (v_i) and (v_j) must be the improper ideal (1) for every index $j \neq i$, by the monotony law for join in lattices, and therefore $v_i + v_j = 1$ whenever $i \neq j$, by Corollary 8.18. Thus, (ii)(b) holds, and therefore so does (iii)(b).

To verify (iii)(c), consider an arbitrary system $(r_i : i \in I)$ of elements in $\mathfrak{A}$ with $r_i \leq u_i$ for each i. The given system of principal ideals is assumed to be orthogonal, so there must be an element s in $\mathfrak{A}$ such that

$$s/(v_i) = r_i/(v_i) \tag{1}$$

for each i. The quotient $\mathfrak{A}/(v_i)$ is isomorphic to the relativization $\mathfrak{A}(u_i)$ via the function φ that maps each coset $p/(v_i)$ to the product $p \cdot u_i$, by Theorem 10.3 and the assumption that $u_i = -v_i$ (which implies, in particular, that $u_i \equiv 1 \mod v_i$, and therefore

$$p \cdot u_i \equiv p \cdot 1 \equiv p \mod v_i,$$

so that the cosets of $p \cdot u_i$ and of p modulo (v_i) coincide for each index i). The cosets on the left and right sides of (1) are respectively mapped to the elements $s \cdot u_i$ and $r_i \cdot u_i$ by this isomorphism, so the condition in (1) is equivalent to the condition

$$s \cdot u_i = r_i \cdot u_i \tag{2}$$

for each i. Use Boolean algebra, the condition in (iii)(a) (which has already been shown to be a consequence of (i)), (2), and the assumption that r_i is below u_i, to arrive at

$$s = s \cdot 1 = s \cdot (\textstyle\sum_i u_i) = \sum_i s \cdot u_i = \sum_i r_i \cdot u_i = \sum_i r_i.$$

Thus, condition (iii)(c) holds. This completes the proof of the implication from (i) to (iii).

To establish the reverse implication, assume that the conditions in (iii) hold, with the goal of deriving (i). Since (iii)(a) implies (ii)(a), the intersection of the system of ideals in (i) must be the trivial ideal, by (ii)(a) and Lemma 8.19(ii).

To prove that the system in (i) satisfies the second condition in the definition of a system of orthogonal ideals, consider an arbitrary system $(r_i : i \in I)$ of elements in $\mathfrak{A}$. The sum

$$s = \textstyle\sum_i r_i \cdot u_i \tag{3}$$

exists in $\mathfrak{A}$, by condition (iii)(c). For each index i, the equation in (2) holds, by (3), condition (iii)(b), and Boolean algebra:

$$s \cdot u_i = (\textstyle\sum_j r_j \cdot u_j) \cdot u_i = \sum_j (r_j \cdot u_j \cdot u_i) = r_i \cdot u_i \cdot u_i = r_i \cdot u_i.$$

It has already been observed that (2) is equivalent to (1), so the second orthogonality condition does hold. □

The preceding lemma leads naturally to the definition of an orthogonal system of ideal elements.

Definition 11.28. A system $(u_i : i \in I)$ of ideal elements in a relation algebra $\mathfrak{A}$ is said to be *orthogonal* if it satisfies the following conditions.

(i) $\sum_i u_i = 1$.
(ii) $u_i \cdot u_j = 0$ for $i \neq j$.
(iii) Whenever $(r_i : i \in I)$ is a system of elements in $\mathfrak{A}$ with $r_i \leq u_i$ for each i, the sum $\sum_i r_i$ exists in $\mathfrak{A}$. □

The first two conditions say that the ideal elements partition the unit of $\mathfrak{A}$. (It is allowed that some of the elements u_i in this partition are zero.) The third condition says that certain (possibly infinite) sums must exist, namely those sums in which the ith summand is below u_i for each index i (see Figure 11.2). We shall say that a system of ideal elements has the *supremum property* if it satisfies the third condition.

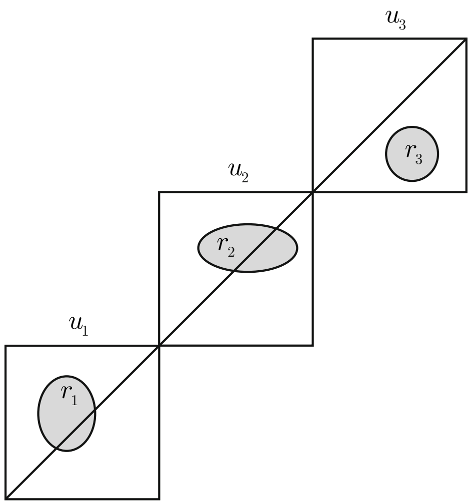


Fig. 11.2 An orthogonal system of ideal elements u_1, u_2, u_3.

When the index set I is finite—that is to say, when there are only finitely many ideal elements in the system— the supremum property holds automatically.

Corollary 11.29. *A finite system of ideal elements in an arbitrary relation algebra is orthogonal if and only if it partitions the unit.*

Similarly, when the relation algebra under discussion is complete, the supremum property holds automatically.

Corollary 11.30. *An arbitrary system of ideal elements in a complete relation algebra is orthogonal if and only if it partitions the unit.*

We are at last ready for the external version of the *Product Decomposition Theorem*, which is a generalization of Theorem 11.11.

Theorem 11.31. *A relation algebra $\mathfrak{A}$ is isomorphic to a product $\prod_{i \in I} \mathfrak{A}_i$ if and only if there exists an orthogonal system $(u_i : i \in I)$ of ideal elements in $\mathfrak{A}$ such that $\mathfrak{A}(u_i)$ is isomorphic to $\mathfrak{A}_i$ for each i.*

Proof. The relation algebra $\mathfrak{A}$ is isomorphic to the product $\prod_{i \in I} \mathfrak{A}_i$ if and only if there exists an orthogonal system $(v_i : i \in I)$ of ideal elements in $\mathfrak{A}$ such that the quotient $\mathfrak{A}/(v_i)$ is isomorphic to the factor $\mathfrak{A}_i$ for each index i, by Corollary 11.26 and the remarks following the corollary. Write $u_i = -v_i$, and observe that the quotient $\mathfrak{A}/(v_i)$ is isomorphic to the relativization $\mathfrak{A}(u_i)$, by Theorem 10.3. Consequently, $\mathfrak{A}/(v_i)$ and $\mathfrak{A}_i$ are isomorphic if and only if $\mathfrak{A}(u_i)$ and $\mathfrak{A}_i$ are isomorphic. Finally, $((v_i) : i \in I)$ is an orthogonal system of ideals if and only if $(u_i : i \in I)$ is an orthogonal system of ideal elements, by Lemma 11.27 and Definition 11.28. Combine these observations to arrive at the desired conclusion. □

The preceding theorem assumes a particularly simple form in two special, but important, cases, namely when the decomposition is finite and when the underlying relation algebra is complete. In these cases, the requirement that the supremum property hold is superfluous, by Corollaries 11.29 and 11.30.

Corollary 11.32. *A relation algebra $\mathfrak{A}$ is isomorphic to the product of a finite system $(\mathfrak{A}_i : i \in I)$ of relation algebras if and only if there exists a finite system $(u_i : i \in I)$ of ideal elements partitioning the unit in $\mathfrak{A}$ such that $\mathfrak{A}(u_i)$ is isomorphic to $\mathfrak{A}_i$ for each i.*

Notice that the preceding corollary applies in particular to all finite relation algebras.

Corollary 11.33. *A complete relation algebra $\mathfrak{A}$ is isomorphic to the product of an arbitrary system $(\mathfrak{A}_i : i \in I)$ of relation algebras if and only if there exists a system $(u_i : i \in I)$ of ideal elements partitioning the unit in $\mathfrak{A}$ such that $\mathfrak{A}(u_i)$ is isomorphic to $\mathfrak{A}_i$ for each i.*

11.9 Internal products of systems

If $(\mathfrak{A}_i : i \in I)$ is a system of set relation algebras $\mathfrak{A}_i$ with units E_i and mutually disjoint base sets U_i, then the product $\mathfrak{A} = \prod_i \mathfrak{A}_i$ is naturally represented as a set relation algebra with unit and base set

$$E = \bigcup_i E_i \qquad \text{and} \qquad U = \bigcup_i U_i$$

respectively. In fact, the function that assigns to each element R in $\mathfrak{A}$ the relation $\bigcup_i R_i$ on U is an embedding of $\mathfrak{A}$ into $\mathfrak{Re}(E)$. (Recall in this connection that an element R in $\mathfrak{A}$ is a function on I such that R_i belongs to $\mathfrak{A}_i$, and is therefore a relation on U_i, for each index i. In particular, it makes sense to form the union $\bigcup_i R_i$.) The argument is very similar to the argument for the binary case given at the beginning of Section 11.4, and is left as an exercise.

This representation of a product of set relation algebras as a set relation algebra motivates a more general internal product construction.

Definition 11.34. A relation algebra $\mathfrak{A}$ is an *internal product* of a system $(\mathfrak{A}_i : i \in I)$ of relation algebras if it satisfies the following conditions.

(i) The universe of $\mathfrak{A}_i$ is included in $\mathfrak{A}$ for every index i.
(ii) Every sum $\sum_i r_i$, with r_i in $\mathfrak{A}_i$ for each i, exists in $\mathfrak{A}$.
(iii) Every element r in $\mathfrak{A}$ can be written in exactly one way as a sum $r = \sum_i r_i$ with r_i in $\mathfrak{A}_i$ for each i.
(iv) For any two such sums $\sum_i r_i$ and $\sum_i s_i$ in $\mathfrak{A}$, the following equations hold:

$$(\textstyle\sum_i r_i) + (\sum_i s_i) = \sum_i (r_i + s_i), \qquad -(\sum_i r_i) = \sum_i -r_i,$$
$$(\textstyle\sum_i r_i) ; (\sum_i s_i) = \sum_i (r_i ; s_i), \qquad (\sum_i r_i)^{\smile} = \sum_i r_i^{\smile},$$

and the identity element in $\mathfrak{A}$ is the sum (in $\mathfrak{A}$) of the identity elements in the algebras $\mathfrak{A}_i$. (In each of these equations, the operations on the left sides are performed in $\mathfrak{A}$, and those on the right—apart from the summations over the indices i—are performed in $\mathfrak{A}_i$.) $\square$

If $\mathfrak{A}$ is an internal product of the system $(\mathfrak{A}_i : i \in I)$, then the algebras $\mathfrak{A}_i$ are called *internal factors* of $\mathfrak{A}$. An element r in an internal product $\mathfrak{A}$ has the form $r = \sum_i r_i$ for some necessarily unique elements r_i in the factor algebras $\mathfrak{A}_i$, by condition (iii) in the preceding definition; the element r_i is called the ith *component* of r. The

conditions in part (iv) of the definition say that the operations in the internal product are performed componentwise in the factor algebras. This implies that the defined operations and distinguished elements in $\mathfrak{A}$ are also determined componentwise; in particular

$$(\sum_i r_i) \cdot (\sum_i s_i) = \sum_i (r_i \cdot s_i), \qquad (\sum_i r_i) \dotplus (\sum_i s_i) = \sum_i (r_i \dotplus s_i),$$

and zero, one, and the diversity element in $\mathfrak{A}$ are respectively the sums in $\mathfrak{A}$ over all indices i, of the zeros, ones, and diversity elements in the factor algebras $\mathfrak{A}_i$.

As in the binary case, three questions arise immediately. First, what is the relationship between internal and external products? Second, to what extent are internal products uniquely determined? And third, under what conditions do internal products exists? The answers to these questions are similar to the answers that were given in the binary case (see Section 11.4).

As regards the first question, there is a canonical isomorphism from the external product of a system of relation algebras to an internal product of the system: it is the function φ defined by

$$\varphi(r) = \sum_i r_i$$

for each element $r = (r_i : i \in I)$ in the external product (where the sum on the right is formed in the internal product). The function φ is well defined and has as its domain the entire universe of the external product because of conditions (i) and (ii) in Definition 11.34; it is one-to-one and onto because of condition (iii); and it preserves the operations and the distinguished element of the product because of condition (iv). As an example of how these arguments proceed in detail, here is the proof that φ preserves relative multiplication. Consider elements

$$r = (r_i : i \in I) \qquad \text{and} \qquad s = (s_i : i \in I)$$

in the external product, and let $t = (t_i : i \in I)$ be the element in the external product that is determined by $t_i = r_i \,;\, s_i$ (in $\mathfrak{A}_i$) for each index i. Thus, $t = r \,;\, s$ in the external product, by the definition of relative multiplication in the external product. Use this observation, the definition of φ, and condition (iv) to obtain

$$\begin{aligned}\varphi(r \,;\, s) = \varphi(t) = \sum_i t_i = \sum_i (r_i \,;\, s_i)& \\ = (\sum_i r_i) \,;\, (\sum_i s_i) = \varphi(r) \,;\, \varphi(s).&\end{aligned}$$

Turn now to the second question. Two internal products, say $\mathfrak{A}_1$ and $\mathfrak{A}_2$, of a system of relation algebras are always isomorphic via a mapping that is the identity on the universes of the factor algebras. In fact, if φ_1 and φ_2 are the canonical isomorphisms from the external product to $\mathfrak{A}_1$ and $\mathfrak{A}_2$ respectively, then the composition $\varphi = \varphi_2 \circ \varphi_1^{-1}$ maps $\mathfrak{A}_1$ isomorphically onto $\mathfrak{A}_2$, and maps each element in a factor algebra to itself. This isomorphism justifies speaking of *the* internal product of the relation algebras.

The answer to the third question is that the internal product of a system $(\mathfrak{A}_i : i \in I)$ of relation algebras exists if and only if (the universes of) the algebras are mutually disjoint except for a common zero. The proof of this assertion, though not deep, is somewhat longer than the preceding arguments and is facilitated by a preliminary analysis of the external product

$$\mathfrak{B} = \prod_i \mathfrak{A}_i$$

of the system.

For each fixed index i, let $u^{(i)}$ be the element in $\mathfrak{B}$ whose ith coordinate is the unit of $\mathfrak{A}_i$ and whose jth coordinate for $j \neq i$ is the zero element in $\mathfrak{A}_j$. Each coordinate in $u^{(i)}$ is an ideal element in the corresponding factor algebra, so $u^{(i)}$ is an ideal element in $\mathfrak{B}$ (see the remarks following Lemma 11.18). It is not difficult to check that the system$(u^{(i)} : i \in I)$ satisfies the conditions in Definition 11.28 for being an orthogonal system of ideal elements in $\mathfrak{B}$. Indeed, the ith coordinate of $u^{(i)}$ is the unit of $\mathfrak{A}_i$, so the sum $\sum_i u^{(i)}$ is the element in $\mathfrak{B}$ that has the unit of $\mathfrak{A}_i$ as its ith coordinate for every index i. In other words, the sum is the unit of $\mathfrak{B}$. Similarly, the elements $u^{(i)}$ and $u^{(j)}$ are disjoint when $i \neq j$, because the product of these two elements is the element in $\mathfrak{B}$ whose kth coordinate, for every index k, is the product of the kth coordinates of $u^{(i)}$ and $u^{(j)}$, and one of these two coordinates is always zero. Finally, suppose $(r^{(i)} : i \in I)$ is a system of elements in $\mathfrak{B}$ such that $r^{(i)} \leq u^{(i)}$ for each i. This inequality and the definition of $u^{(i)}$ imply that the jth coordinate of $r^{(i)}$ is the zero element of $\mathfrak{A}_j$ for every index $j \neq i$. Consequently, the sum $\sum_i r^{(i)}$ is the element in $\mathfrak{B}$ whose ith coordinate coincides with the ith coordinate of $r^{(i)}$ for each index i. In particular, this sum exists in $\mathfrak{B}$.

Let $\mathfrak{B}_i$ be the relativization of $\mathfrak{B}$ to the ideal element $u^{(i)}$. Thus, the elements in $\mathfrak{B}_i$ are just the elements in $\mathfrak{B}$ whose jth coordinate, for each index $j \neq i$, is the zero element in $\mathfrak{A}_j$. Using the orthogonality established in the preceding paragraph, one can show that $\mathfrak{B}$ is the

internal product of the system $(\mathfrak{B}_i : i \in I)$. Since this assertion follows immediately from Theorem 11.39 in the next section, we shall not give a separate verification of it now. The algebras $\mathfrak{B}_i$ are obviously mutually disjoint except for a common zero element, which is the zero element in $\mathfrak{B}$, because the elements $u^{(i)}$ and $u^{(j)}$ are disjoint for $i \neq j$.

Return now to the problem of when the internal product $\mathfrak{A}$ of a system $(\mathfrak{A}_i : i \in I)$ of relation algebras exists. Assume first that $\mathfrak{A}$ does exist. It is to be shown that the algebras in the given system are disjoint except for a common zero, which is the zero element in $\mathfrak{A}$. To this end, it suffices to show that the canonical isomorphism φ from $\mathfrak{B}$ to $\mathfrak{A}$ maps the internal factor $\mathfrak{B}_i$ (of $\mathfrak{B}$) onto the internal factor $\mathfrak{A}_i$ (of $\mathfrak{A}$). Once this is accomplished, the desired result about the factors $\mathfrak{A}_i$ follows from the corresponding result about the factors $\mathfrak{B}_i$ that was noted at the end of the preceding paragraph. The canonical isomorphism φ maps each element r in $\mathfrak{B}$ to the sum of the coordinates of r. Each element r in $\mathfrak{B}_i$ has zero as its jth coordinate for $j \neq i$, so φ must map r to its ith coordinate. In other words, φ maps $\mathfrak{B}_i$ into $\mathfrak{A}_i$. For each element t in $\mathfrak{A}_i$, the element in $\mathfrak{B}$ whose ith coordinate is t and whose other coordinates are zero belongs to $\mathfrak{B}_i$ and is mapped by φ to t, so φ maps $\mathfrak{B}_i$ onto $\mathfrak{A}_i$. Since the operations in $\mathfrak{B}$ and in $\mathfrak{A}$ are performed coordinatewise and componentwise respectively, it follows that φ actually maps $\mathfrak{B}_i$ isomorphically to $\mathfrak{A}_i$.

Assume finally that the algebras in the system $(\mathfrak{A}_i : i \in I)$ are mutually disjoint except for a common zero element. It is to be shown that the internal product $\mathfrak{A}$ of the system really does exist. Let φ_i be the function from $\mathfrak{A}_i$ to $\mathfrak{B}_i$ that maps each element r in $\mathfrak{A}_i$ to the element $\hat{r}$ in $\mathfrak{B}$ whose ith coordinate is r and whose other coordinates are all zero. It is easy to check that φ_i is an isomorphism. For example, to see that φ_i preserves the operation of relative multiplication, consider elements r and s in $\mathfrak{A}_i$, and write $t = r \,;\, s$. The relative product of the image elements $\hat{r}$ and $\hat{s}$ in $\mathfrak{B}$, and therefore also in the relativization $\mathfrak{B}_i$, is $\hat{t}$, because the operations in $\mathfrak{B}$ are performed coordinatewise, and the coordinates of $\hat{r}$ and $\hat{s}$ are all zero, except for the ith coordinates. Consequently,

$$\varphi_i(r \,;\, s) = \varphi_i(t) = \hat{t} = \hat{r} \,;\, \hat{s} = \varphi_i(r) \,;\, \varphi_i(s).$$

The isomorphisms in the system $(\varphi_i : i \in I)$ agree on the common zero element of the algebras $\mathfrak{A}_i$, since this zero element is mapped by each of them to the zero element of $\mathfrak{B}$ (which is the same as the zero element of $\mathfrak{B}_i$). With the exception of this common zero element, the

isomorphisms in the system map their domains to sets that are disjoint (except for a common zero), because the range algebras $\mathfrak{B}_i$ are disjoint except for a common zero, by the preliminary observations made above. An argument similar to the Exchange Principle (Theorem 7.15) allows us to replace the relativization $\mathfrak{B}_i$ in $\mathfrak{B}$ with the algebra $\mathfrak{A}_i$ for each index i, provided that the elements in $\mathfrak{B}$ that do not occur in any of the internal factors $\mathfrak{B}_i$ are first replaced with new elements that do not occur in any of the algebras $\mathfrak{A}_i$. The result is an algebra $\mathfrak{A}$ that is isomorphic to $\mathfrak{B}$ via a mapping that agrees with φ_i on each set A_i. Since $\mathfrak{B}$ is the internal product of the system $(\mathfrak{B}_i : i \in I)$, it follows that $\mathfrak{A}$ must be the internal product of the system $(\mathfrak{A}_i : i \in I)$.

The observations of the preceding paragraphs are summarized in the following *Existence and Uniqueness Theorem* for internal products, which generalizes Theorem 11.14.

Theorem 11.35. *The internal product of a system $(\mathfrak{A}_i : i \in I)$ of relation algebras exists if and only if the algebras in the system are mutually disjoint except for a common zero. If the internal product exists, then it is unique up to isomorphisms that are the identity functions on the factor algebras; and the mapping $(r_i : i \in I) \longmapsto \sum_i r_i$ is an isomorphism from the external product to the internal product of the system.*

There is really no loss of generality in assuming that a given system of relation algebras is disjoint except for a common zero element. Given any system of relation algebras, one can always pass to a system of isomorphic copies that has the required disjointness property, and then form the internal product of these copies. In what follows, we shall always assume (tacitly) that any system of relation algebras for which the internal product is being formed has the required disjointness property.

As was mentioned at the end of Section 11.5, whether one uses external or internal products is partly a matter of taste; they are two sides of the same coin. There are, however, situations in which it seems preferable to use internal products, because the formulations of the results are more straightforward and sometimes even sharper than the analogous results for external products.

Here are some examples. The first is the analogue of the characterization of ideal elements in an external product that was given informally after Lemma 11.18. It is related to the description of ideal elements in relativizations that is contained in Lemma 10.9.

Corollary 11.36. *The ideal elements in the internal product of a system of relation algebras are just the sums of ideal elements from the factor algebras. In particular, the ideal element atoms in the internal product are just the ideal element atoms in the factor algebras.*

The next example is the analogue of Lemma 11.22 for internal products, and it is related to the description of atoms in relativizations that is contained in Lemma 10.5.

Corollary 11.37. *The atoms in the internal product of a system of relation algebras are just the atoms in the factor algebras. The product is atomic if and only if each factor algebra is atomic.*

The version of Lemma 11.23 for internal products is perhaps only a bit more natural than its external version.

Corollary 11.38. *Suppose $\mathfrak{A}$ is the internal product of a system of relation algebras $(\mathfrak{A}_i : i \in I)$, and u_i is the unit of $\mathfrak{A}_i$ for each i. The supremum of a subset X of $\mathfrak{A}$ exists in $\mathfrak{A}$ if and only if the supremum of the set*

$$X_i = \{s \cdot u_i : s \in X\}$$

exists in $\mathfrak{A}_i$ for each i. If these suprema exist, say r_i is the supremum of X_i in $\mathfrak{A}_i$, then $r = \sum_i r_i$ is the supremum of X in $\mathfrak{A}$. The internal product $\mathfrak{A}$ is complete if and only if each of its factors is complete.

In subsequent sections, we shall give further examples of results that have simpler and sharper formulations for internal products than they have for external products. For relation algebras, it definitely seems easier to work with internal rather than external products. Consequently, from now on, when we speak of a product of relation algebras, we shall usually mean an internal product.

11.10 General internal decompositions

The observations of the preceding section establish a close relationship between external and internal products. Every result about external products has an analogue for internal products, and vice versa. The most important of these analogues is the following internal version of the Product Decomposition Theorem 11.31.

Theorem 11.39. *A relation algebra $\mathfrak{A}$ is the internal product of a system $(\mathfrak{A}_i : i \in I)$ of algebras if and only if there is an orthogonal system $(u_i : i \in I)$ of ideal elements in $\mathfrak{A}$ such that $\mathfrak{A}(u_i) = \mathfrak{A}_i$ for each index i.*

Proof. One way to prove this theorem is to derive it from the external version of the theorem, with the help of the canonical isomorphism from an external to an internal product. We follow a more direct, but longer route that clarifies the roles of the various conditions in the definitions of an internal product and an orthogonal system of ideal elements.

Assume first that there exists an orthogonal system

$$(u_i : i \in I) \tag{1}$$

of ideal elements in $\mathfrak{A}$ with the property that

$$\mathfrak{A}(u_i) = \mathfrak{A}_i \tag{2}$$

for each i. In order to prove that $\mathfrak{A}$ is the internal product of the algebras $\mathfrak{A}_i$, conditions (i)–(iv) in Definition 11.34 must be verified.

The assumption in (2) implies that the universe of $\mathfrak{A}_i$ is a subset of $\mathfrak{A}$ for each index i, so condition (i) holds. To verify condition (ii), suppose $(r_i : i \in I)$ is a system of elements with the property that r_i is in $\mathfrak{A}_i$ for each i. The element r_i is below u_i, by (2), and the system in (1) is orthogonal, by assumption, so the sum $\sum_i r_i$ exists in $\mathfrak{A}$, by the definition of an orthogonal system (see Definition 11.28(iii)).

To verify condition (iii), consider an arbitrary element r in $\mathfrak{A}$, and put $r_i = r \cdot u_i$ for each i. The assumption in (2) implies that r_i belongs to $\mathfrak{A}_i$. The system in (1) sums to 1, by the orthogonality of the system (see Definition 11.28(i)), so

$$r = r \cdot 1 = r \cdot (\textstyle\sum_i u_i) = \sum_i (r \cdot u_i) = \sum_i r_i .$$

Thus, r can be written as a sum of elements r_i in $\mathfrak{A}_i$. To check that this representation of r is unique, suppose $r = \sum_i s_i$, where s_i is in $\mathfrak{A}_i$ for each i. The element s_i belongs to $\mathfrak{A}$ and is below u_i, by (2). The orthogonality of the system in (1) implies that $u_j \cdot u_i = 0$ for each $j \neq i$ (see Definition 11.28(ii)), and therefore

$$r_j \cdot u_i = \begin{cases} 0 & \text{if} \quad j \neq i, \\ r_i & \text{if} \quad j = i, \end{cases} \qquad \text{and} \qquad s_j \cdot u_i = \begin{cases} 0 & \text{if} \quad j \neq i, \\ s_i & \text{if} \quad j = i. \end{cases} \tag{3}$$

Consequently,

$$r_i = \sum_j (r_j \cdot u_i) = (\sum_j r_j) \cdot u_i = r \cdot u_i$$
$$= (\sum_j s_j) \cdot u_i = \sum_j (s_j \cdot u_i) = s_i$$

for each i, by (3) and Boolean algebra. Conclusion: every element in $\mathfrak{A}$ can be written in exactly one way as a sum of elements r_i from $\mathfrak{A}_i$, so condition (iii) holds.

The verifications of the equations in condition (iv) are all rather similar in spirit. Here, for instance, is the verification of the third equation. Suppose that

$$r = \sum_i r_i \qquad \text{and} \qquad s = \sum_i s_i, \tag{4}$$

where r_i and s_i are in $\mathfrak{A}_i$ for each i. Observe that r_i and s_i are both in $\mathfrak{A}$ and below u_i, by (2). If $i \neq j$, then in $\mathfrak{A}$ we have

$$r_i \,;\, s_j \leq u_i \,;\, u_j = u_i \cdot u_j = 0, \tag{5}$$

by the monotony law for relative multiplication, Lemma 5.41(ii), and the assumption that the system in (1) is an orthogonal system of ideal elements (see, in particular, Definition 11.28(ii)). Consequently,

$$r \,;\, s = (\sum_i r_i) \,;\, (\sum_i s_i) = \sum_{ij} (r_i \,;\, s_j) = \sum_i (r_i \,;\, s_i)$$

in $\mathfrak{A}$, by (4), the complete distributivity of relative multiplication, and (5). The relative product of r_i and s_i on the right is formed in $\mathfrak{A}$, but this product coincides with the relative product of the two elements in $\mathfrak{A}_i$, by (2) and the definition relative multiplication in a relativization. This completes the proof that $\mathfrak{A}$ is the internal product of the given system of algebras.

To prove the converse direction of the theorem, assume that $\mathfrak{A}$ is the internal product of the given system of algebras. For each index i, let u_i be the unit of $\mathfrak{A}_i$. It is to be shown that the resulting system (1) is orthogonal and (2) holds. Again, we shall need to refer several times to conditions (i)–(iv) in Definition 11.34.

Condition (iv) implies that the unit 1 of $\mathfrak{A}$ must be the sum of the units of the individual factors, that is to say,

$$1 = \sum_i u_i \tag{6}$$

(see the remarks following Definition 11.34). Condition (iv) also implies that u_i and u_j must be disjoint when $i \neq j$. In more detail, for each index k, define elements r_k and s_k in $\mathfrak{A}_k$ by

$$r_k = \begin{cases} 0 & \text{if} \quad k \neq i, \\ u_i & \text{if} \quad k = i, \end{cases} \qquad \text{and} \qquad s_k = \begin{cases} 0 & \text{if} \quad k \neq j, \\ u_j & \text{if} \quad k = j, \end{cases} \tag{7}$$

and observe that

$$u_i = \textstyle\sum_k r_k \qquad \text{and} \qquad u_j = \textstyle\sum_k s_k. \tag{8}$$

The analogue for multiplication of the equations in condition (iv) (see the remarks following Definition 11.34) implies that

$$u_i \cdot u_j = \textstyle\sum_k (r_k \cdot s_k), \tag{9}$$

where the multiplications on the right are performed in the factor algebras $\mathfrak{A}_k$. At least one of r_k and s_k is always zero, so the product of these two factors is always zero. Condition (iv) also implies that the zero element in $\mathfrak{A}$ is the sum of the zero elements of the factor algebras (see the remarks following Definition 11.34), so it may be concluded from (7) and the preceding remarks that $u_i \cdot u_j = 0$ in $\mathfrak{A}$. Thus, $(u_i : i \in I)$ is a partition of the unit of $\mathfrak{A}$.

To check that u_i is indeed an ideal element in $\mathfrak{A}$, consider the elements r_k defined on the left side of (7), and observe that the first equation in (8) holds. Use (6), (8), and the third equation in condition (iv) to obtain

$$1 ; u_i ; 1 = (\textstyle\sum_k u_k) ; (\textstyle\sum_k r_k) ; (\textstyle\sum_k u_k) = \textstyle\sum_k (u_k ; r_k ; u_k),$$

where the relative multiplications on the right are performed in the factor algebras $\mathfrak{A}_k$. For $k \neq i$, we have $r_k = 0$ and therefore

$$u_k ; r_k ; u_k = 0,$$

by Corollary 4.17 and its first dual applied to the factor $\mathfrak{A}_k$. On the other hand,

$$u_i ; r_i ; u_i = u_i ; u_i ; u_i = u_i,$$

by (7), the assumption that u_i is the unit of $\mathfrak{A}_i$, and Lemma 4.5(iv) applied to the factor $\mathfrak{A}_i$. Combine these observations to conclude that the equation $1 ; u_i ; 1 = u_i$ holds in $\mathfrak{A}$.

In order to complete the proof that (1) is an orthogonal system, it must be shown that the supremum property holds. Before doing this, we verify the equation in (2). Conditions (i), (iii), and (iv) imply that the universe of $\mathfrak{A}_i$ coincides with that of $\mathfrak{A}(u_i)$. Indeed, if s is in $\mathfrak{A}_i$,

then s is in $\mathfrak{A}$, by condition (i), and s is below u_i because u_i is the unit of $\mathfrak{A}_i$, so s is in $\mathfrak{A}(u_i)$. To establish the reverse inclusion, suppose that s belongs to $\mathfrak{A}(u_i)$. The element s is then in $\mathfrak{A}$, so for each index k there must be an element s_k in $\mathfrak{A}_k$ such that $s = \sum_k s_k$, by condition (iii). Let r_k be defined as in (7), and observe that the first equation in (8) holds. Use the fact that s is below u_i, by assumption, and apply the analogue for multiplication of the equations in condition (iv), to obtain

$$s = u_i \cdot s = (\textstyle\sum_k r_k) \cdot (\sum_k s_k) = \sum_k (r_k \cdot s_k), \tag{10}$$

where the multiplications on the right are performed in the factor algebras $\mathfrak{A}_k$. For $k \neq i$, the factor r_k is zero, so the product $r_k \cdot s_k$ is zero. On the other hand, u_i is the unit in $\mathfrak{A}_i$, and the component s_i is an element in $\mathfrak{A}_i$, so s_i is below u_i and therefore

$$r_i \cdot s_i = u_i \cdot s_i = s_i$$

in $\mathfrak{A}_i$. Combine these observations with (10) to conclude that $s = s_i$ and therefore that s belongs to $\mathfrak{A}_i$. Thus, $\mathfrak{A}_i$ and $\mathfrak{A}(u_i)$ have the same universe.

Analogous arguments show that the operations of $\mathfrak{A}_i$ coincide with those of $\mathfrak{A}(u_i)$. For instance, if elements r and s are in $\mathfrak{A}(u_i)$, then they belong to $\mathfrak{A}$ and we can write them as

$$r = \textstyle\sum_j r_j \qquad \text{and} \qquad s = \sum_j s_j,$$

where $r_i = r$ and $s_i = s$, and $r_j = s_j = 0$ for $j \neq i$. Apply the third equation in condition (iv) to arrive at

$$r \mathbin{;} s = (\textstyle\sum_j r_j) \mathbin{;} (\sum_j s_j) = \sum_j r_j \mathbin{;} s_j = r_i \mathbin{;} s_i = r \mathbin{;} s,$$

where the first two relative multiplications are performed in $\mathfrak{A}$ and therefore also in $\mathfrak{A}(u_i)$, and the last two are performed in $\mathfrak{A}_i$. Thus, relative multiplication in $\mathfrak{A}(u_i)$ coincides with relative multiplication in $\mathfrak{A}_i$. Similar arguments apply to the other operations, so the two algebras have the same operations, and therefore (2) holds.

Return now to the problem of verifying the supremum property for the system in (1). Suppose that $(r_i : i \in I)$ is a system of elements in $\mathfrak{A}$ with $r_i \leq u_i$ for each i. The element r_i belongs to $\mathfrak{A}(u_i)$, by the definition of this relativization, and therefore r_i belongs to $\mathfrak{A}_i$, by the observations of the preceding paragraphs. Apply condition (ii) to see that the sum $\sum_i r_i$ exists in $\mathfrak{A}$. Conclusion: the system in (1) has the supremum property and is therefore orthogonal. □

A representation of a relation algebra $\mathfrak{A}$ as the internal product of a system of relation algebras is called an *internal direct decomposition* of $\mathfrak{A}$.

The preceding theorem implies the following *Relativization Decomposition Theorem*.

Theorem 11.40. *In a relation algebra $\mathfrak{A}$, if $(e_i : i \in I)$ is a system of disjoint equivalence elements with the property that $\sum_i r_i$ exists whenever $r_i \leq e_i$ for each i, then the sum $e = \sum_i e_i$ exists and is an equivalence element, and the relativization $\mathfrak{A}(e)$ is the internal product of the system of relativizations $(\mathfrak{A}(e_i) : i \in I)$.*

Proof. The sum e of the given system of equivalence elements

$$(e_i : i \in I) \tag{1}$$

exists, by the assumption that the system in (1) has the supremum property. Since this system is also assumed to be disjoint, e is an equivalence element in $\mathfrak{A}$, by Lemma 5.23, so it makes sense to speak of the relativization of $\mathfrak{A}$ to e. If $i \neq j$, then

$$e_i \,;\, e_j = 0, \tag{2}$$

by Lemma 5.22 and the assumed disjointness of the system in (1), and therefore

$$\begin{aligned} e \,;\, e_i \,;\, e = (\textstyle\sum_j e_j) \,;\, e_i \,;\, (\textstyle\sum_j e_j) = \textstyle\sum_{j,k}(e_j \,;\, e_i \,;\, e_k)& \\ = e_i \,;\, e_i \,;\, e_i = e_i,& \end{aligned} \tag{3}$$

by the definition of e, the complete distributivity of relative multiplication, (2), and Lemma 5.8(ii). The computation in (3) shows that e_i is an ideal element in $\mathfrak{A}(e)$.

The system in (1) is disjoint, by assumption, it sums to the unit e in $\mathfrak{A}(e)$, by the definition of e and Lemma 10.6, and it has the supremum property in $\mathfrak{A}(e)$, by the hypotheses of the theorem and Lemma 10.6, so it satisfies the conditions of Definition 11.28 for being an orthogonal system of ideal elements in $\mathfrak{A}(e)$. Apply Theorem 11.39 to conclude that $\mathfrak{A}(e)$ is the internal product of the system of relativizations $(\mathfrak{A}(e_i) : i \in I)$. □

In the preceding theorem, if the relation algebra $\mathfrak{A}$ is complete or the system of equivalence elements is finite, then the condition that the sum $\sum_i r_i$ exists whenever $r_i \leq e_i$ for each i is automatically satisfied.

11.11 Total decompositions

An external or internal direct decomposition of a relation algebra $\mathfrak{A}$ is said to be *total* if each of the factor algebras in the decomposition is directly indecomposable in the sense that it is non-degenerate and cannot itself be decomposed into a product of two non-degenerate relation algebras. We have already seen in Theorem 9.12 that a relation algebra is directly indecomposable if and only if it is simple (see also the related remarks at the end of Section 11.3), so a direct decomposition is total if and only if each of the factor algebras in the decomposition is simple. The existence of a total decomposition of $\mathfrak{A}$ simplifies substantially the structural analysis of $\mathfrak{A}$.

A relation algebra $\mathfrak{A}$ is said to have a *unique* total (external or internal) decomposition if it has a total decomposition into the product of a system $(\mathfrak{A}_i : i \in I)$ of simple relation algebras, and if for every other such decomposition $(\mathfrak{B}_j : j \in J)$ of $\mathfrak{A}$, there is a bijection ϑ from the index set I to the index set J such that $\mathfrak{A}_i$ is isomorphic to $\mathfrak{B}_{\vartheta(i)}$ for each i in the external case, and $\mathfrak{A}_i$ is equal to $\mathfrak{B}_{\vartheta(i)}$ for each i in the internal case. Not every relation algebra $\mathfrak{A}$ has a total decomposition, but when such a decomposition does exist, it is always unique.

The following *Total Decomposition Theorem* characterizes when a relation algebra has a total decomposition.

Theorem 11.41. *A relation algebra $\mathfrak{A}$ has a total direct decomposition if and only if the Boolean algebra of ideal elements in $\mathfrak{A}$ is atomic and the system of distinct ideal element atoms has the supremum property. If a total decomposition of $\mathfrak{A}$ exists, then it is unique and the factors of the decomposition are just the relativizations of $\mathfrak{A}$ to the various ideal element atoms.*

Proof. It is notationally more convenient to prove the internal version of the theorem. According to the internal version of the Product Decomposition Theorem 11.39 and the observations made above, a relation algebra $\mathfrak{A}$ has total direct decomposition if and only if there exists an orthogonal system

$$(u_i : i \in I) \tag{1}$$

of ideal elements in $\mathfrak{A}$ such that the relativizations $\mathfrak{A}(u_i)$ are all simple. If such a system of ideal elements exists, then the factors of the

decomposition are just those relativizations. These requirements translate into the following four conditions on the system in (1), by Definition 11.28 and Corollary 10.10. First, $\sum_i u_i = 1$. Second, $u_i \cdot u_j = 0$ whenever $i \neq j$. Third, the system has the supremum property in $\mathfrak{A}$. Fourth, u_i is an atom in the Boolean algebra B of ideal elements in $\mathfrak{A}$.

Assume that (1) is a system of ideal element atoms in $\mathfrak{A}$, so that the fourth condition is automatically satisfied. The second condition holds just in case the ideal element atoms u_i and u_j are distinct when $i \neq j$. The first condition holds just in case the Boolean algebra B is atomic, and the system in (1) contains all of the atoms in B. Combine these observations to conclude that $\mathfrak{A}$ has a total decomposition if and only if the Boolean algebra B of ideal elements is atomic, and the system of ideal element atoms in (1) lists all of the ideal element atoms in B without repetitions, and also has the supremum property. This completes the proof of the first assertion of the theorem.

To prove the second assertion of the theorem, suppose that $\mathfrak{A}$ does have a total (internal) decomposition, determined say by the system of ideal element atoms in (1). Any other total decomposition of $\mathfrak{A}$ must be given by an orthogonal system

$$(v_j : j \in J) \tag{2}$$

of ideal elements, and the factors of this decomposition are just the relativizations $\mathfrak{A}(v_j)$, by Theorem 11.39. The systems in (1) and (2) must both enumerate the distinct atoms in B, by the observations of the preceding paragraphs, so there must be a bijection ϑ from I to J such that $u_i = v_{\vartheta(i)}$ for each i. It follows that

$$\mathfrak{A}(u_i) = \mathfrak{A}(v_{\vartheta(i)})$$

for each i, so the total decomposition of $\mathfrak{A}$ is unique. □

A direct decomposition of a relation algebra is said to be *finite* if the system of factor algebras is finite. The preceding theorem easily implies the following characterization of when a relation algebra has a finite total direct decomposition.

Corollary 11.42. *A relation algebra $\mathfrak{A}$ has a finite total direct decomposition if and only if there are only finitely many ideal elements in $\mathfrak{A}$.*

Proof. A relation algebra $\mathfrak{A}$ has a total direct decomposition into the direct product of finitely many simple factor algebras if and only if the

Boolean algebra of ideal elements in $\mathfrak{A}$ is atomic with finitely many atoms, by Theorem 11.41. (The requirement that the system of distinct ideal element atoms possess the supremum property is unnecessary in this case, because a finite system of distinct ideal element atoms automatically has the supremum property, as finite sums always exist in a relation algebra.) The Boolean algebra of ideal elements in $\mathfrak{A}$ is atomic with finitely many atoms if and only if it is finite, that is to say, if and only if there are only finitely many ideal elements in $\mathfrak{A}$, by Boolean algebra. □

A concrete example may help to illuminate the Total Decomposition Theorem. Consider an equivalence relation E on a non-empty set U, and suppose that $(U_i : i \in I)$ is an enumeration without repetitions of the distinct equivalence classes of E. Take $\mathfrak{A}$ to be the full set relation algebra on the equivalence relation E, so that $\mathfrak{A} = \mathfrak{Re}(E)$. It is not difficult to check that the ideal elements in $\mathfrak{A}$ are just the unions of Cartesian squares of equivalence classes, which are the sets of the form

$$\bigcup_{i\in J} U_i \times U_i,$$

where J ranges over the subsets of I. The Boolean algebra of ideal

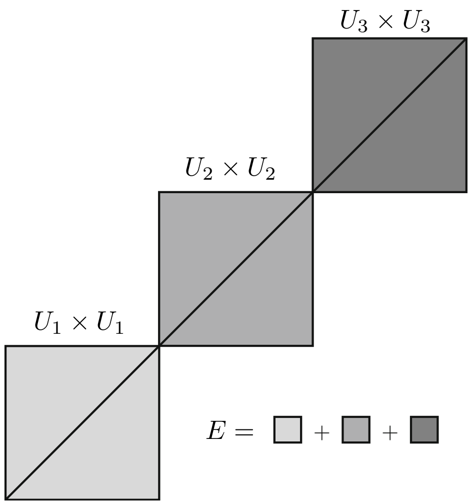


Fig. 11.3 The total decomposition of $\mathfrak{Re}(E)$ when E is an equivalence relation with three equivalence classes.

elements in $\mathfrak{A}$ is atomic, and its atoms are the squares $U_i \times U_i$, that is

to say, its atoms are the squares that have equivalence classes of E as their sides. Consequently, the system

$$(U_i \times U_i : i \in I)$$

is an enumeration without repetitions of the distinct ideal element atoms in $\mathfrak{A}$, and this system has the supremum property because $\mathfrak{A}$ is complete. Apply the Total Decomposition Theorem to conclude that $\mathfrak{A}$ has a unique total decomposition into the internal product of the relativizations $\mathfrak{A}(U_i \times U_i)$. As has already been pointed out several times, these relativization coincide with the full set relation algebras $\mathfrak{Re}(U_i)$ on the equivalence classes U_i. Thus, we arrive at the following *Decomposition Theorem for* $\mathfrak{Re}(E)$ (see Figure 11.3).

Theorem 11.43. *Suppose E is an equivalence relation on a non-empty set, and $(U_i : i \in I)$ is a listing without repetitions of the equivalence classes of E. The full set relation algebra $\mathfrak{Re}(E)$ has a unique total decomposition into the internal product of the system of full set relation algebras $(\mathfrak{Re}(U_i) : i \in I)$.*

In particular, a full set relation algebra $\mathfrak{Re}(E)$ has a finite total decomposition if and only if the equivalence relation E has just finitely many equivalence classes (see Corollary 11.42).

The preceding theorem may be viewed as a special case of the following more general result, called the *Atomic Decomposition Theorem.*

Theorem 11.44. *A complete relation algebra with an atomic Boolean algebra of ideal elements always has a unique total direct decomposition.*

Proof. The system of distinct ideal element atoms in the given relation algebra has the supremum property because the relation algebra is assumed to be complete. Apply Theorem 11.41 to arrive at the desired conclusion. □

Actually, Theorem 11.41 implies more than what is stated in Theorem 11.44. If $(u_i : i \in I)$ is a listing without repetitions of the distinct ideal element atoms in a complete relation algebra $\mathfrak{A}$ with an atomic Boolean algebra of ideal elements, then $\mathfrak{A}$ can be written in a unique way (up to permutations of factors) as the internal product of the system of relativizations $(\mathfrak{A}(u_i) : i \in I)$, and each of these relativizations is a simple relation algebra. Moreover, $\mathfrak{A}$ is atomic if and only if each of the relativizations $\mathfrak{A}(u_i)$ is atomic, by Corollary 11.37.

Lemma 8.28 ensures that an atomic relation algebra has an atomic Boolean algebra of ideal elements. Consequently, the preceding theorem applies to all complete and atomic relation algebras, and in particular to all finite relation algebras.

Corollary 11.45. *Every complete and atomic relation algebra has a unique total direct decomposition.*

Theorem 11.44 and its corollary are very important because they reduce the study of complete and atomic relation algebras to the study of complete and atomic relation algebras that are *simple*. In some sense, the hypothesis that the relation algebra be complete and atomic does not severely restrict the applicability of the theorem, because—as we shall see later—every relation algebra can be extended to a complete and atomic relation algebra. The theorem is of no help, however, in analyzing the structure of simple relation algebras. There are, however, a series of constructions that are similar in spirit to direct products and direct decompositions, and can be applied to analyze and construct simple relation algebras (see, for example, [51], [34], and [37]).

The preceding theorem gives some sufficient conditions for a total decomposition of a relation algebra to exist. At the other extreme, it may be concluded from Theorem 11.41 that if a relation algebra $\mathfrak{A}$ has a non-zero ideal element below which there are no ideal element atoms, and in particular if the Boolean algebra of ideal elements is non-degenerate and atomless, then $\mathfrak{A}$ has no total decomposition.

As it turns out, it is always possible to decompose a complete relation algebra into the product of two factors, the first of which is uniquely decomposable into a product of simple factors, and the second of which has no ideal element atoms—and therefore no simple factors—whatsoever. This is the content of the following *Complete Decomposition Theorem.*

Theorem 11.46. *A complete relation algebra $\mathfrak{A}$ always has a unique internal direct decomposition $\mathfrak{A} = \mathfrak{A}_1 \otimes \mathfrak{A}_2$ such that $\mathfrak{A}_1$ has a unique total direct decomposition, and $\mathfrak{A}_2$ has no ideal element atoms and is therefore atomless and has no simple factors at all.*

Proof. Let u be the sum of the set of ideal element atoms in $\mathfrak{A}$. This sum exists in $\mathfrak{A}$, by the assumption that $\mathfrak{A}$ is complete, and it is an ideal element, by Lemma 5.39(ii). The ideal elements in the relativization $\mathfrak{A}(u)$ are the ideal elements in $\mathfrak{A}$ that are below u, and in particular, the ideal element atoms in $\mathfrak{A}(u)$ are the ideal element atoms

in $\mathfrak{A}$ that are below u, by Lemma 10.9. Thus, every ideal element atom from $\mathfrak{A}$ belongs to $\mathfrak{A}(u)$ and is an ideal element atom in $\mathfrak{A}(u)$, by the definition of u. Also, u is the sum of these ideal element atoms, not only in $\mathfrak{A}$, but also in $\mathfrak{A}(u)$, by Lemma 10.6. Since u is the unit of $\mathfrak{A}(u)$ and is the sum of the ideal element atoms, the Boolean algebra of ideal elements in $\mathfrak{A}(u)$ must be atomic. Also $\mathfrak{A}(u)$ is complete, by the assumption that $\mathfrak{A}$ is complete and Lemma 10.6. Consequently, $\mathfrak{A}(u)$ has a unique total direct decomposition, by the Atomic Decomposition Theorem 11.44.

The complement of u is also an ideal element in $\mathfrak{A}$, in view of Lemma 5.39(iv). There are no ideal element atoms in $\mathfrak{A}$ that are below $-u$, by the definition of u, so there can be no ideal element atoms in the relativization $\mathfrak{A}(-u)$, by Lemma 10.9. Thus, the Boolean algebra of ideal elements in $\mathfrak{A}(-u)$ must be atomless. From this it follows that $\mathfrak{A}(-u)$ itself must be atomless. Indeed, if r were an atom in this relativization, then r would be an atom in $\mathfrak{A}$, by Lemma 10.5, and therefore $1\,;r\,;1$ would be an ideal element atom in $\mathfrak{A}$, by Lemma 8.28. Since

$$1\,;r\,;1 \leq 1\,;-u\,;1 = -u,$$

it would follow that $\mathfrak{A}(-u)$ has an ideal element atom, in contradiction to what has already been shown.

The algebra $\mathfrak{A}$ is the internal product of $\mathfrak{A}(u)$ and $\mathfrak{A}(-u)$, by the Product Decomposition Theorem 11.15. Put

$$\mathfrak{A}_1 = \mathfrak{A}(u) \qquad \text{and} \qquad \mathfrak{A}_2 = \mathfrak{A}(-u), \tag{1}$$

to arrive at an internal direct decomposition of $\mathfrak{A}$ with the required properties.

Suppose now that $\mathfrak{A} = \mathfrak{B}_1 \otimes \mathfrak{B}_2$ is any internal decomposition of $\mathfrak{A}$ with the required properties. It is to be shown that

$$\mathfrak{B}_1 = \mathfrak{A}_1 \qquad \text{and} \qquad \mathfrak{B}_2 = \mathfrak{A}_2. \tag{2}$$

There must be an ideal element v in $\mathfrak{A}$ such that

$$\mathfrak{B}_1 = \mathfrak{A}(v) \qquad \text{and} \qquad \mathfrak{B}_2 = \mathfrak{A}(-v), \tag{3}$$

by Theorem 11.15. Since $\mathfrak{B}_1$ is totally decomposable, by assumption, the Boolean algebra of ideal elements in $\mathfrak{A}(v)$ must be atomic, by (3) and the Total Decomposition Theorem 11.41. The unit v of this relativization must therefore be the sum of the ideal element atoms

in $\mathfrak{A}(v)$, by Boolean algebra. Consequently, v must be a sum of ideal element atoms in $\mathfrak{A}$, by Lemmas 10.6 and 10.9. The factor $\mathfrak{B}_2$ contains no ideal element atoms at all, by assumption, so every ideal element atom in $\mathfrak{A}$ must belong to $\mathfrak{A}(v)$, by (3) and Corollary 11.36. It follows that v is the sum in $\mathfrak{A}$ of all of the ideal element atoms in $\mathfrak{A}$, so $v = u$ and $-v = -u$, where u is the element defined at the beginning of the proof. Combine this observation with (1) and (3) to conclude that (2) holds. □

11.12 Atomless Boolean algebras of ideal elements

The conclusions of the Complete Decomposition Theorem 11.46 raise the problem of whether there actually are relation algebras with atomless Boolean algebras of ideal elements, and if so, how examples of such algebras might be constructed. Of course, atomless Boolean algebras, converted into Boolean relation algebras, provide trivial examples. The purpose of this section is to construct a rather general and more interesting class of examples.

The first step is to construct an infinite binary tree of subsets of a fixed infinite set I, using standard methods. (The restriction to binary trees is not essential, but it helps to simplify notation and to communicate the main ideas more clearly.) Here is one possible approach. For each natural number n, let 2^n be the set of all n-termed sequences of zeros and ones. When $n = 0$, there is only one such sequence, namely the empty sequence $\varnothing$, and we take $I_\varnothing$ to be I. Suppose now that I_α has been defined for every sequence α in 2^n. Each such sequence α has two extensions to sequences β and γ in 2^{n+1}: both extensions agree with α on natural numbers $i < n$, and $\beta(n) = 0$, while $\gamma(n) = 1$. Take I_β and I_γ to be any partition of I_α into infinite sets; thus, these two sets are infinite, disjoint, and have I_α as their union. A straightforward argument by induction on n shows that the sets I_α for α in 2^n form a partition of I.

Fix an arbitrary non-degenerate relation algebra $\mathfrak{A}$. The second step in the construction is to correlate with each element r in the direct (external) power $\mathfrak{A}^{2^n}$ an element $\hat{r}$ in the direct power $\mathfrak{A}^I$. Essentially, $\hat{r}$ is obtained by concatenating a sufficient number of copies of r with itself. More precisely, the elements in $\mathfrak{A}^{2^n}$ are functions with domain 2^n that take their values in $\mathfrak{A}$. Given such a function r, define $\hat{r}$ by

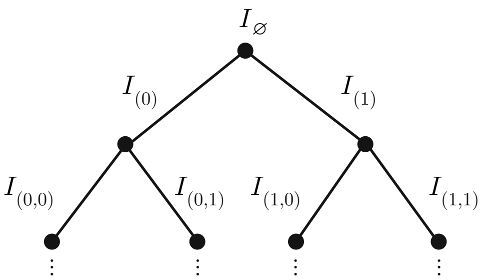


Fig. 11.4 The binary tree of subsets of I.

$$\hat{r}(i) = r(\alpha) \qquad \text{if and only if} \qquad i \in I_\alpha$$

for every argument i in I and every α in 2^n.

To give some concrete examples of this correlation, consider first the case when $n = 0$. In this case, r is a function with the empty sequence $\varnothing$ as the only element in its domain, and the value of r at $\varnothing$ is some element p in $\mathfrak{A}$. The correlated element in $\mathfrak{A}^I$ is the constant function $\hat{r}$ on I that assumes the value p at every i in I. If I is the set of natural numbers, then $\hat{r}$ is the constant sequence

$$(p, p, p, p, \dots).$$

Consider next the case when $n = 1$. In this case, r is a function with the sequences of length one, (0) and (1), as the only elements in its domain, and the values of r on these sequences are elements p and q in $\mathfrak{A}$. The correlated element in $\mathfrak{A}^I$ is the function $\hat{r}$ on I defined by

$$\hat{r}(i) = \begin{cases} p & \text{if} \quad i \in I_{(0)}, \\ q & \text{if} \quad i \in I_{(1)}. \end{cases}$$

If I is the set of natural numbers, and if $I_{(0)}$ and $I_{(1)}$ are the sets of even and odd natural numbers respectively, then $\hat{r}$ is the sequence

$$(p, q, p, q, \dots).$$

The third step in the construction is the definition, for each natural number n, of a subuniverse B_n of $\mathfrak{A}^I$. It consists of elements of the form $\hat{r}$ for r in $\mathfrak{A}^{2^n}$. Clearly, B_n contains the identity element in $\mathfrak{A}^I$, because the identity element is just $\hat{r}$, where r is the identity element in $\mathfrak{A}^{2^n}$, that is to say, r is the function that assumes the identity

element of $\mathfrak{A}$ as its value at each sequence in 2^n. Also, B_n is closed under the operations of addition, complement, relative multiplication, and converse, because these operations are defined coordinatewise in both $\mathfrak{A}^I$ and $\mathfrak{A}^{2^n}$. In more detail,

$$\begin{aligned} \hat{r} + \hat{s} &= \hat{t}, &\qquad &\text{where} &\qquad t &= r + s, \\ -\hat{r} &= \hat{t}, &\qquad &\text{where} &\qquad t &= -r, \\ \hat{r} \mathbin{;} \hat{s} &= \hat{t}, &\qquad &\text{where} &\qquad t &= r \mathbin{;} s, \\ \hat{r}^{\smile} &= \hat{t}, &\qquad &\text{where} &\qquad t &= r^{\smile}, \end{aligned}$$

where the operations on the left are performed in $\mathfrak{A}^I$, and those on the right are performed in $\mathfrak{A}^{2^n}$. Since $\mathfrak{A}^{2^n}$ is closed under the aforementioned operations, so is B_n. Write $\mathfrak{B}_n$ for the subalgebra of $\mathfrak{A}^I$ with universe B_n. This subalgebra is isomorphic to $\mathfrak{A}^{2^n}$ via the function that maps $\hat{r}$ to r for each element r in $\mathfrak{A}^{2^n}$. Consequently, $\mathfrak{B}_n$ inherits all of the properties of $\mathfrak{A}^{2^n}$. In particular, $\hat{r}$ is an ideal element in $\mathfrak{B}_n$ if and only if r is an ideal element in $\mathfrak{A}^{2^n}$.

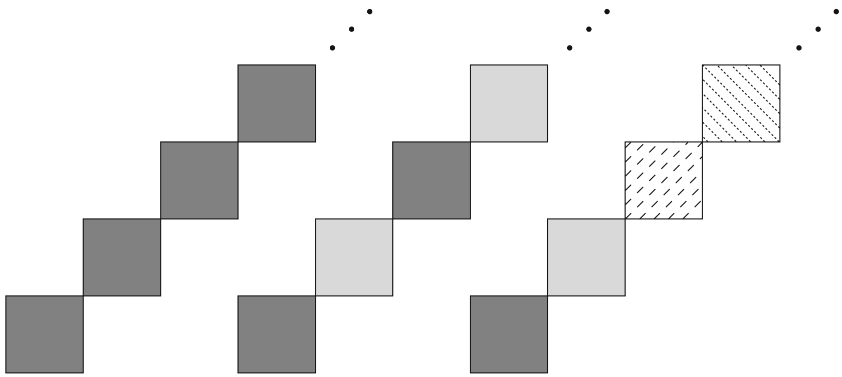


Fig. 11.5 Schematic of the algebras $\mathfrak{B}_0$, $\mathfrak{B}_1$, and $\mathfrak{B}_2$.

Every element in $\mathfrak{B}_n$ belongs to $\mathfrak{B}_{n+1}$ as well. To prove this, fix an element r in $\mathfrak{A}^{2^n}$, and let s be the element in $\mathfrak{A}^{2^{n+1}}$ that is essentially obtained by concatenating r with itself. More precisely,

$$s(\beta) = r(\alpha) \qquad \text{and} \qquad s(\gamma) = r(\alpha),$$

for each α in 2^n, where β and γ are the two extensions of α in 2^{n+1}. The element $\hat{s}$ in $\mathfrak{B}_{n+1}$ that is correlated with s is defined by

$$\hat{s}(i) = s(\beta) \qquad \text{and} \qquad \hat{s}(i) = s(\gamma)$$

for i in I_β and in I_γ respectively. Since $s(\beta)$ and $s(\gamma)$ both coincide with $r(\alpha)$, and since I_α is the union of I_β and I_γ, the preceding definition may be condensed to

$$\hat{s}(i) = r(\alpha) \quad \text{if and only if} \qquad i \in I_\alpha,$$

and this is just the definition of $\hat{r}$ in $\mathfrak{B}_n$. Thus, the element $\hat{r}$ in $\mathfrak{B}_n$ coincides with the element $\hat{s}$ in $\mathfrak{B}_{n+1}$. The operations in $\mathfrak{B}_n$ and $\mathfrak{B}_{n+1}$ are, by definition, restrictions of the corresponding operations of $\mathfrak{A}^I$, so $\mathfrak{B}_n$ must be a subalgebra of $\mathfrak{B}_{n+1}$ (see Figure 11.5).

Each non-zero element $\hat{r}$ in $\mathfrak{B}_n$ is split in $\mathfrak{B}_{n+1}$ into the sum of two disjoint non-zero elements. To see this, fix a non-zero element r in $\mathfrak{A}^{2^n}$, and define elements t and u in $\mathfrak{A}^{2^{n+1}}$ as follows: for every given element α in 2^n, if β and γ are the two extensions of α in 2^{n+1} that are mentioned above, put

$$t(\beta) = r(\alpha), \qquad t(\gamma) = 0, \qquad u(\beta) = 0, \qquad u(\gamma) = r(\alpha).$$

Observe that t and u are non-zero because r is non-zero, they are disjoint because at least one of $t(\rho)$ and $u(\rho)$ is zero for each ρ in 2^{n+1}, and they sum to the element s that is defined in terms of r in the preceding paragraph, by the definition of s and the fact that one of $t(\rho)$ and $u(\rho)$ is $r(\alpha)$, and the other is 0, for each ρ in 2^{n+1}. These observations and the remarks above imply that $\hat{t}$ and $\hat{u}$ are non-zero, disjoint elements in $\mathfrak{B}_{n+1}$ that sum to $\hat{s}$. Since $\hat{s}$ coincides with $\hat{r}$, we can write $\hat{r}$ as the disjoint sum of the non-zero elements $\hat{t}$ and $\hat{u}$. Notice, in particular, that if r is a non-zero ideal element in $\mathfrak{A}^{2^n}$, then t and u are non-zero ideal elements in $\mathfrak{A}^{2^{n+1}}$ and therefore the non-zero ideal element $\hat{r}$ in $\mathfrak{B}_n$ is split in $\mathfrak{B}_{n+1}$ into the sum of the two disjoint non-zero ideal elements $\hat{t}$ and $\hat{u}$.

The sequence $\mathfrak{B}_0$, $\mathfrak{B}_1$, $\mathfrak{B}_2$, ... forms a strictly ascending chain of subalgebras of $\mathfrak{A}^I$ with the property that each non-zero element in $\mathfrak{B}_n$ is split into a sum of two disjoint non-zero elements in $\mathfrak{B}_{n+1}$, and each non-zero ideal element in $\mathfrak{B}_n$ is split into a sum of two disjoint non-zero ideal elements in $\mathfrak{B}_{n+1}$. The union of this chain is therefore a subalgebra of $\mathfrak{A}^I$ that has no atoms and no ideal element atoms, and that, as a bonus, inherits many of the properties of the original relation algebra $\mathfrak{A}$. This fact will prove useful later on. Here is a summary of what has been obtained.

Theorem 11.47. *If $\mathfrak{A}$ is a non-degenerate relation algebra, and I an infinite set, then the union of the chain $\mathfrak{B}_0$, $\mathfrak{B}_1$, $\mathfrak{B}_2$, ... of subalgebras of $\mathfrak{A}^I$ constructed above is an atomless subalgebra of $\mathfrak{A}^I$ with no ideal element atoms.*

11.13 Decompositions of homomorphisms

The existence of an internal direct decomposition of a relation algebra raises the question of whether homomorphisms on the algebra admit similar decompositions. As it turns out, under certain restrictions, such decompositions are possible. To motivate the discussion, we begin with a stronger version of Lemma 11.21 that applies to internal products.

Lemma 11.48. *Suppose $\mathfrak{A}$ and $\mathfrak{B}$ are internal products of systems of relation algebras $(\mathfrak{A}_i : i \in I)$ and $(\mathfrak{B}_i : i \in I)$ respectively, and φ_i is a mapping from $\mathfrak{A}_i$ to $\mathfrak{B}_i$ for each i. The mapping φ from $\mathfrak{A}$ to $\mathfrak{B}$ defined on each element $r = \sum_i r_i$ in $\mathfrak{A}$ by*

$$\varphi(r) = \textstyle\sum_i \varphi_i(r_i)$$

is a homomorphism if and only if φ_i is a homomorphism for every i. If the mappings are homomorphisms, then φ is an extension of φ_i for each i, and φ is one-to-one or onto or complete just in case each of the mappings φ_i is one-to-one or onto or complete respectively.

Proof. To give a sense of how the proofs of these assertions proceed for internal products, here is the argument that φ preserves relative multiplication if and only if the mappings φ_i all preserve relative multiplication. Suppose

$$r = \textstyle\sum_i r_i \qquad \text{and} \qquad s = \textstyle\sum_i s_i \tag{1}$$

are elements in $\mathfrak{A}$. We have $r \,;\, s = \sum_i r_i \,;\, s_i$, by condition (iv) in Definition 11.34, so

$$\varphi(r \,;\, s) = \textstyle\sum_i \varphi_i(r_i \,;\, s_i), \tag{2}$$

by the definition of φ. Similarly,

$$\varphi(r) \,;\, \varphi(s) = (\textstyle\sum_i \varphi_i(r_i)) \,;\, (\textstyle\sum_i \varphi_i(s_i)) = \textstyle\sum_i(\varphi_i(r_i) \,;\, \varphi_i(s_i)), \tag{3}$$

by the definition of φ and by condition (iv) in Definition 11.34 applied to the internal product $\mathfrak{B}$. If each of the mappings φ_i preserves relative multiplication, then

$$\varphi_i(r_i \,;\, s_i) = \varphi_i(r_i) \,;\, \varphi_i(s_i) \tag{4}$$

for each i, and therefore

$$\varphi(r \,;\, s) = \varphi(r) \,;\, \varphi(s), \tag{5}$$

by (2)–(4). On the other hand, if φ preserves relative multiplication, then

$$\textstyle\sum_i \varphi_i(r_i \,;\, s_i) = \sum_i(\varphi_i(r_i) \,;\, \varphi_i(s_i)),$$

by (2), (3), and (5), and therefore (4) holds, by the uniqueness part of condition (iii) in Definition 11.34 applied to $\mathfrak{B}$.

Assume now that the mappings under discussion are homomorphisms. To prove that the product homomorphism φ is an extension of each homomorphism φ_i, consider an element r in $\mathfrak{A}$, as in (1). If r belongs to the factor $\mathfrak{A}_i$, then $r_i = r$ and $r_j = 0$ for $j \neq i$, by the uniqueness part of condition (iii) in Definition 11.34 applied to $\mathfrak{A}$. Consequently, $\varphi_j(r_j) = \varphi_j(0) = 0$ for $j \neq i$, by the homomorphism properties of φ_j, and therefore

$$\varphi(r) = \textstyle\sum_j \varphi_j(r_j) = \varphi_i(r_i) = \varphi_i(r),$$

by the definition of φ. Thus, φ and φ_i agree on $\mathfrak{A}_i$. □

The mapping φ defined in the preceding lemma might be called the *internal product* of the system of mappings $(\varphi_i : i \in I)$. The lemma is stronger than its external version, Lemma 11.21, because it asserts that an (internal) product homomorphism is actually an extension of each of the factor homomorphisms. A corresponding assertion would not be true in the framework of external products.

We now work toward a kind of converse to Lemma 11.48 that turns out to be quite useful, namely a decomposition theorem for certain homomorphisms on internal products. Consider the internal product $\mathfrak{A}$ of a system of relation algebras $(\mathfrak{A}_i : i \in I)$. A homomorphism φ from $\mathfrak{A}$ into an arbitrary relation algebra $\mathfrak{B}$ is said to *preserve the supremum property* if for every element $r = \sum_i r_i$ in $\mathfrak{A}$, with r_i in $\mathfrak{A}_i$ for each i, we have $\varphi(r) = \sum_i \varphi(r_i)$ in $\mathfrak{B}$. Preserving the supremum property is weaker than being complete (as a homomorphism), since

a complete homomorphism preserves all existing suprema, and not just the suprema of systems of elements from distinct factors. More concretely, if the index set I is finite, then every homomorphism φ on $\mathfrak{A}$ automatically preserves the supremum property, because φ preserves all finite sums; but φ may not preserve all existing suprema in $\mathfrak{A}$.

Suppose φ is an epimorphism from $\mathfrak{A}$ to $\mathfrak{B}$ that preserves the supremum property. The Product Decomposition Theorem 11.39 applied to $\mathfrak{A}$ ensures the existence of an orthogonal system $(u_i : i \in I)$ of ideal elements in $\mathfrak{A}$ such that $\mathfrak{A}_i = \mathfrak{A}(u_i)$ for each i. The system of images $(v_i : i \in I)$, where $v_i = \varphi(u_i)$, is readily seen to be an orthogonal system of ideal elements in $\mathfrak{B}$. Indeed, a homomorphism maps ideal elements to ideal elements, so each v_i is an ideal element in $\mathfrak{B}$. Also, a homomorphism maps disjoint elements to disjoint elements, so v_i and v_j are disjoint for $i \neq j$. Furthermore,

$$1 = \varphi(1) = \varphi(\textstyle\sum_i u_i) = \sum_i \varphi(u_i) = \sum_i v_i,$$

because $1 = \sum_i u_i$ and φ is a homomorphism that preserves the supremum property. Thus, the system of ideal elements $(v_i : i \in I)$ is a partition of the unit in $\mathfrak{B}$.

The verification that this system has the supremum property involves a bit more work. Let $(s_i : i \in I)$ be a system of elements in $\mathfrak{B}$ such that $s_i \leq v_i$ for each i. It is to be shown that the supremum $\sum_i s_i$ exists in $\mathfrak{B}$. The assumption that φ is an epimorphism implies that there must be a system $(t_i : i \in I)$ of elements in $\mathfrak{A}$ such that $\varphi(t_i) = s_i$ for each i. Now the element t_i may not belong to the factor $\mathfrak{A}_i$, but the product $r_i = t_i \cdot u_i$ does belong to $\mathfrak{A}_i$, because r_i is in the relativization $\mathfrak{A}(u_i)$, and this relativization coincides with $\mathfrak{A}_i$. Consequently, the supremum $r = \sum_i r_i$ exists in $\mathfrak{A}$, because the system $(u_i\,; i \in I)$ is assumed to be orthogonal and therefore has the supremum property. Moreover, φ maps r_i to v_i, since

$$\varphi(r_i) = \varphi(t_i \cdot u_i) = \varphi(t_i) \cdot \varphi(u_i) = s_i \cdot v_i = s_i,$$

by the definition of r_i, the homomorphism properties of φ, the assumptions on t_i and v_i, and the assumption that s_i is below v_i. Therefore,

$$\varphi(r) = \varphi(\textstyle\sum_i r_i) = \sum_i \varphi(r_i) = \sum_i s_i,$$

by the assumption that φ preserves the supremum property. Conclusion: $\varphi(r)$ is the supremum of the system $(s_i : i \in I)$ in $\mathfrak{B}$.

It has been shown that $(v_i : i \in I)$ is an orthogonal system of ideal elements in $\mathfrak{B}$. Write $\mathfrak{B}_i = \mathfrak{B}(v_i)$ for each i, and apply Theorem 11.39 to conclude that $\mathfrak{B}$ is the internal product of the system $(\mathfrak{B}_i : i \in I)$.

Let φ_i be the restriction of the homomorphism φ to the factor $\mathfrak{A}_i$, and observe that φ_i maps $\mathfrak{A}_i$ into $\mathfrak{B}_i$. Indeed, for any element r in $\mathfrak{A}_i$, we have $r \leq u_i$, because $\mathfrak{A}_i$ is the relativization $\mathfrak{A}(u_i)$, and therefore

$$\varphi_i(r) = \varphi(r) \leq \varphi(u_i) = v_i,$$

by the definition of φ_i, the homomorphism properties of φ, and the definition of v_i. Consequently, $\varphi_i(r)$ belongs to $\mathfrak{B}_i$, by the definition of $\mathfrak{B}_i$. Notice also that for any element $r = \sum r_i$ in $\mathfrak{A}$, we have

$$\varphi(r) = \varphi(\textstyle\sum_i r_i) = \sum_i \varphi(r_i) = \sum_i \varphi_i(r_i),$$

by the assumption that φ preserves the supremum property and by the definition of the mappings φ_i. Since φ is an epimorphism satisfying the preceding equalities, we may apply Lemma 11.48 to conclude that φ_i is an epimorphism from $\mathfrak{A}_i$ to $\mathfrak{B}_i$ for each i, and that φ is the internal product of the system of epimorphisms $(\varphi_i : i \in I)$.

The above decomposition of φ into the internal product of factor epimorphisms is unique with respect to the given representation of the domain algebra $\mathfrak{A}$ as the internal product of the system $(\mathfrak{A}_i : i \in I)$. More precisely, if ψ_i is an epimorphism from $\mathfrak{A}_i$ to some algebra $\mathfrak{C}_i$ for each i, and if φ is the internal product of the system $(\psi_i : i \in I)$, then ψ_i coincides with φ_i, and $\mathfrak{C}_i$ coincides with $\mathfrak{B}_i$, for each i. Indeed, for any element r in $\mathfrak{A}_i$, we have

$$\psi_i(r) = \varphi(r) = \varphi_i(r),$$

by the assumption that φ is the internal product of both systems of mappings, and therefore φ is an extension of both ψ_i and φ_i for each i. We summarize the preceding discussion in the following *First Homomorphism Decomposition Theorem.*

Theorem 11.49. *Let $\mathfrak{A}$ be the internal product of a system of relation algebras $(\mathfrak{A}_i : i \in I)$. If an epimorphism φ from $\mathfrak{A}$ to a relation algebra $\mathfrak{B}$ preserves the supremum property, then $\mathfrak{B}$ can be decomposed into the internal product of a system of relation algebras $(\mathfrak{B}_i : i \in I)$, and φ can be decomposed in a unique way into the internal product of a system of mappings $(\varphi_i : i \in I)$ such that φ_i is an epimorphism from $\mathfrak{A}_i$ to $\mathfrak{B}_i$ for each i.*

As was mention earlier, when the index set I in the preceding theorem is finite, every epimorphism on the internal product $\mathfrak{A}$ preserves the supremum property. The theorem assumes a simpler form in this case because the hypothesis concerning the preservation of the supremum property may be dropped.

In the preceding theorem, epimorphisms from a product of relation algebras into an arbitrary relation algebra are decomposed into products of factor epimorphisms. In the dual situation, a homomorphism φ from an arbitrary relation algebra into a product of relation algebras is given, and the task is to decompose φ in some reasonable way.

We begin by considering a method of constructing a homomorphism on a relation algebra $\mathfrak{A}$ from a given system $(\varphi_i : i \in I)$ of homomorphisms on $\mathfrak{A}$. In the internal version of this construction, the target algebras $\mathfrak{B}_i$ of the homomorphisms φ_i must be disjoint except for a common zero element. Define a function φ from $\mathfrak{A}$ into the internal product $\mathfrak{B}$ of the system of algebras $(\mathfrak{B}_i : i \in I)$ by putting

$$\varphi(r) = \textstyle\sum_i \varphi_i(r)$$

for each r in $\mathfrak{A}$. It is not difficult to see that φ is a homomorphism from $\mathfrak{A}$ into $\mathfrak{B}$. For example, to check that φ preserves the operation of relative multiplication, consider elements r and s in $\mathfrak{A}$, and observe that

$$\begin{aligned}\varphi(r\,;s) = \textstyle\sum_i \varphi_i(r\,;s) = \textstyle\sum_i(\varphi_i(r)\,;\varphi_i(s))& \\ = (\textstyle\sum_i \varphi_i(r))\,;(\textstyle\sum_i \varphi_i(s)) &= \varphi(r)\,;\varphi(s),\end{aligned}$$

by the definition of φ, the homomorphism properties of the mappings φ_i, and condition (iv) in the definition of an internal product applied to the algebra $\mathfrak{B}$. The preservation under φ of the remaining operations in $\mathfrak{A}$ may be verified in a completely analogous manner. We shall call φ the *internal amalgamation* of the system of homomorphisms $(\varphi_i : i \in I)$. Notice that the index set I is allowed to be empty. In this case, the product $\mathfrak{B}$ is a degenerate relation algebra, and the amalgamation φ is the homomorphism from $\mathfrak{A}$ to $\mathfrak{B}$ that maps every element to zero.

The definition of the amalgamation φ implies that an element r in $\mathfrak{A}$ belongs to the kernel of φ just in case r belongs to the kernel of each homomorphism φ_i. If we write M for the kernel of φ, and M_i for the kernel of φ_i, then this observation can be expressed by the equation

$$M = \bigcap_i M_i .$$

In particular, φ is one-to-one if and only if the intersection of the ideals M_i is the trivial ideal $\{0\}$. Using Corollary 11.38, it is not difficult to show that the homomorphism φ is complete if and only if each of the homomorphisms φ_i is complete. The proof is left as an exercise. The observations so far are summarized in the following lemma.

Lemma 11.50. *The internal amalgamation φ of a system of homomorphisms $(\varphi_i : i \in I)$ on a relation algebra $\mathfrak{A}$ is a homomorphism from $\mathfrak{A}$ into the internal product of the target algebras. The kernel of φ is the intersection of the kernels M_i of the mappings φ_i. The amalgamation is one-to-one if and only if $\bigcap_i M_i = \{0\}$, and it is complete if and only if each φ_i is complete.*

In the external version of the preceding amalgamation construction, it is unnecessary to impose a disjointness condition on the target algebras $\mathfrak{B}_i$. The *external amalgamation* of the system $(\varphi_i : i \in I)$ is the homomorphism φ from $\mathfrak{A}$ into the external product $\prod_i \mathfrak{B}_i$ that is defined by

$$\varphi(r) = (\varphi_i(r) : i \in I)$$

for each r in $\mathfrak{A}$.

Let us now return to the problem of decomposing a homomorphism that maps a relation algebra $\mathfrak{A}$ into the internal product $\mathfrak{B}$ of a system of relation algebras $(\mathfrak{B}_i : i \in I)$. Given such a homomorphism φ, take φ_i to be the composition of φ with the projection homomorphism ψ_i from $\mathfrak{B}$ to $\mathfrak{B}_i$, so that

$$\varphi_i = \psi_i \circ \varphi .$$

The composition φ_i is clearly a homomorphism from $\mathfrak{A}$ to $\mathfrak{B}_i$. For any element r in $\mathfrak{A}$, if φ maps r to an element s in $\mathfrak{B}$, and if $s = \sum_j s_j$ is the unique representation of s as the sum of its components in $\mathfrak{B}$, then

$$\varphi_i(r) = \psi_i(\varphi(r)) = \psi_i(s) = \psi_i(\textstyle\sum_j s_j) = s_i$$

for each index i, by the definitions of the mappings φ_i and ψ_i, and the assumptions on r; and therefore

$$\textstyle\sum_i \varphi_i(r) = \sum_i s_i = s = \varphi(r).$$

Thus, φ is the internal amalgamation of the system $(\varphi_i : i \in I)$. Moreover, this decomposition of φ into an amalgamation of homomorphisms

is unique. Indeed, if ϑ_i is a homomorphism from $\mathfrak{A}$ to $\mathfrak{B}_i$ for each i, and if $\varphi(r) = \sum_i \vartheta_i(r)$ for each r, then

$$\sum_i \vartheta_i(r) = \sum_i \varphi_i(r)$$

for each r. Use the uniqueness of the representation of elements in $\mathfrak{B}$ as sums of components to conclude that $\vartheta_i(r) = \varphi_i(r)$ for each index i and each element r in $\mathfrak{A}$, and therefore $\vartheta_i = \varphi_i$ for each i. In view of the definition of the mapping φ_i, it is natural to refer to φ_i as the ith *projection* of the homomorphism φ. The preceding observations are summarized in the following *Second Homomorphism Decomposition Theorem*.

Theorem 11.51. *If φ is a homomorphism from a relation algebra into the internal product of a system of relation algebras, then φ is the amalgamation of the system of its projections, and this representation of φ as the amalgamation of a system of homomorphisms into the factor algebras is unique.*

Every homomorphism on a simple relation algebra is either a monomorphism or has a degenerate (one-element) range algebra. Consequently, the preceding theorem has the following sharper form when the domain algebra is simple.

Corollary 11.52. *If φ is an embedding of a simple relation algebra $\mathfrak{A}$ into the product of a system $(\mathfrak{B}_i : i \in I)$ of non-degenerate relation algebras, then the* ith *projection of φ is an embedding of $\mathfrak{A}$ into $\mathfrak{B}_i$ for each i, and φ is the amalgamation of these projections. This representation of φ as the amalgamation of a system of embeddings into the factor algebras is unique.*

11.14 Historical remarks

The origins of the notion of a direct product of algebraic structures can be traced back to the work of René Descartes. The notion of an internal product of groups is in some sense present in a 1846 paper of Johann Peter Gustav Lejeune Dirichlet and in an 1870 paper of Leopold Kronecker. The notion of an internal product of abelian groups is more explicit in the paper [31], published in 1879 by Ferdinand Georg Frobenius and Ludwig Stickelberger, in which it is shown that

every finite abelian group is a product of powers of cyclic subgroups of prime order. Papers by Joseph Henry Maclagan Wedderburn in 1909 and Robert Erich Remak in 1911 on the internal decomposition of finite groups, and later work by others on direct decompositions of groups and groups with operators, inspired Jónsson and Tarski in [52] to study internal decompositions of finite algebras, and to prove a unique direct decomposition theorem in a very general setting. The theorem that every finite relation algebra has a unique total direct decomposition is an immediate consequence of their main theorem.

Tarski's lecture notes [105] from the mid-1940s do not contain any discussion of direct products of relation algebras. An explicit study of direct decompositions of relation algebras appears for the first time in the paper [55] by Jónsson and Tarski, where the Product Decomposition Theorem 11.31 (in its external form) is given, along with its binary version, Theorem 11.11. A general theorem in [21] due to Jónsson, Tarski, and Chen-Chung Chang implies that the class of relation algebras has the refinement property (see Exercise 11.76). The particular proof of the refinement property for relation algebras that is presented in the selected "Hints and Solutions" is due to Givant, as is the proof of the cancellation property for finite relation algebras (see Exercise 11.78). The result in Exercise 11.79 is true for arbitrary finite algebras, and in this general form it is due to László Lovasz [64]; the particular proof of this result for relation algebras that is presented in "Hints and Solutions" is due to Givant. The result in Exercise 11.37 is due to Givant. The presentation in Section 11.8 of the general theory of external decompositions of relation algebras is loosely based on the presentation in Tarski's 1970 lectures [112].

Lemma 11.16 and its binary version, Lemma 11.1, stating that a term definable operation in a direct product is performed coordinatewise, apply to arbitrary algebras, not just relation algebras. The same is true of the assertion that an equation is true in a direct product if and only if it is true in each factor (see Lemmas 11.2 and 11.17), and the related results concerning the preservation of open Horn formulas (see Lemmas 11.3 and 11.18). The preservation of equations under the formation of direct products of algebras was first pointed out in Birkhoff [12]. The theorem that a universal sentence is preserved under binary products if and only if it is equivalent to a universal Horn sentence is essentially due to McKinsey [85] (see Exercise 11.5). More general studies of properties preserved under direct products have been

carried out by Frederick William Galvin in [32] (see also [33]) and Joseph Michael Weinstein in [115].

Similarly, the preservation results in Lemma 11.19, Corollary 11.20, and Lemma 11.21 (and their binary versions in Lemma 11.4, Corollary 11.5, and Lemma 11.6) apply to direct products of systems of arbitrary algebras, not just relation algebras. The results in Lemmas 11.22 and 11.23 are straightforward extensions to relation algebras of well-known results about Boolean algebras.

The notion of the internal product of a system of algebras has been studied for a long time in the context of specific classes of algebras such as groups and modules (see the remarks above). Jónsson and Tarski [52] introduce the notion of internal product for very general classes of algebras that contain among their fundamental operations a binary operation of addition and a zero element. The internal product of a system of relation algebras may be viewed as a special case of their general notion. Internal products of relation algebras are explicitly introduced for the first time in Givant [34]. Theorem 11.35, Product Decomposition Theorem 11.39 (the internal version of the theorem) and the Atomic Decomposition Theorem 11.44 are all stated and proved in [34]. The Total Decomposition Theorem 11.41 and the Complete Decomposition Theorem 11.46 are also due to Givant (the latter is stated and proved in Andréka-Givant [2]), as are the Relativization Decomposition Theorem 11.40 and the Homomorphism Decomposition Theorems 11.49 and 11.51. Lyndon [67] makes a casual, but incorrect, remark that every complete relation algebra is isomorphic to a direct product of simple relation algebras. He applies this remark to reach a somewhat ambiguously formulated conclusion that can be interpreted as asserting the following: every full set relation algebra on an equivalence relation E is isomorphic to the direct product of the system of full set relation algebras on the equivalence classes of E. This is an external version of part of the Decomposition Theorem 11.43 for $\mathfrak{Re}(E)$. A clear statement, with proof, of this observation is given in Tarski's 1970 lectures [112] (see also Maddux [72] and [74]). The construction in Section 11.12 of a class of relation algebras with atomless Boolean algebras of ideal elements dates back to a construction in Givant [34]. A special case of the construction is presented in [2].

Obviously, the definitions and results in Sections 11.1–11.5 may be viewed as special cases of the corresponding definitions and results in

Sections 11.6–11.10. They have been presented separately for pedagogical reasons.

Exercises

11.1. Fill in the missing details in the proof of Lemma 11.1.

11.2. Prove directly (without using Lemma 11.2) that if $\mathfrak{B}$ and $\mathfrak{C}$ are relation algebras, then so is the product $\mathfrak{A} = \mathfrak{B} \times \mathfrak{C}$.

11.3. Prove that a product $\mathfrak{A} = \mathfrak{B} \times \mathfrak{C}$ of relation algebras is commutative or symmetric if and only if both factor algebras $\mathfrak{B}$ and $\mathfrak{C}$ are commutative or symmetric respectively.

11.4. Prove that the product of two non-degenerate relation algebras is never integral and never simple.

11.5. Prove that a universal sentence is preserved under binary products if and only if it is equivalent to a universal Horn sentence (see Section 11.4).

11.6. Prove that a pair (r, s) in a product $\mathfrak{A} = \mathfrak{B} \times \mathfrak{C}$ of relation algebras is an equivalence element if and only if r and s are equivalence elements in the factors $\mathfrak{B}$ and $\mathfrak{C}$ respectively. Prove analogous results for right-ideal elements, subidentity elements, rectangles, and functions.

11.7. Fill in the missing details in the proof of Lemma 11.4.

11.8. Can every subalgebra of a product $\mathfrak{A} = \mathfrak{B} \times \mathfrak{C}$ of relation algebras be decomposed as in Corollary 11.5? In other words, if $\mathfrak{A}_0$ is a subalgebra of $\mathfrak{A}$, are there necessarily subalgebras $\mathfrak{B}_0$ and $\mathfrak{C}_0$ of $\mathfrak{B}$ and $\mathfrak{C}$ respectively such that $\mathfrak{A}_0 = \mathfrak{B}_0 \times \mathfrak{C}_0$?

11.9. Under the hypotheses of Corollary 11.5, prove that $\mathfrak{A}_0 = \mathfrak{B}_0 \times \mathfrak{C}_0$ is a regular subalgebra of $\mathfrak{A} = \mathfrak{B} \times \mathfrak{C}$ if and only if $\mathfrak{B}_0$ and $\mathfrak{C}_0$ are regular subalgebras of $\mathfrak{B}$ and $\mathfrak{C}$ respectively.

11.10. Fill in the missing details in the proof of Lemma 11.6.

11.11. Can every homomorphism ϑ from a product $\mathfrak{A} = \mathfrak{B} \times \mathfrak{C}$ to a product $\mathfrak{A}_0 = \mathfrak{B}_0 \times \mathfrak{C}_0$ of relation algebras be decomposed as in Lemma 11.6? In other words, are there necessarily homomorphisms φ from $\mathfrak{B}$ to $\mathfrak{B}_0$, and ψ from $\mathfrak{C}$ to $\mathfrak{C}_0$, such that

$$\vartheta((r, s)) = (\varphi(r), \psi(s))$$

for every pair (r, s) in $\mathfrak{A}$?

11.12. Consider homomorphisms φ and ψ from a relation algebra $\mathfrak{A}$ to relation algebras $\mathfrak{B}$ and $\mathfrak{C}$ respectively, with kernels M and N respectively. Define a function ϑ from $\mathfrak{A}$ to the product $\mathfrak{B} \times \mathfrak{C}$ by

$$\vartheta(r) = (\varphi(r), \psi(r))$$

for each r in $\mathfrak{A}$. Prove that ϑ is a homomorphism. Prove also that ϑ one-to-one if and only if $M \cap N = \{0\}$. Finally, prove that ϑ is onto if and only if both φ and ψ are onto, and $M + N = A$, where

$$M + N = \{s + t : s \in M \text{ and } t \in N\}.$$

11.13. Suppose M and N are subsets of relation algebras $\mathfrak{B}$ and $\mathfrak{C}$ respectively. Prove that the product $L = M \times N$ is an ideal in $\mathfrak{B} \times \mathfrak{C}$ if and only if M and N are ideals in $\mathfrak{B}$ and $\mathfrak{C}$ respectively.

11.14. If $\mathfrak{A} = \mathfrak{B} \times \mathfrak{C}$ is a product of relation algebras, can every ideal in $\mathfrak{A}$ be written as the product of an ideal in $\mathfrak{B}$ and an ideal in $\mathfrak{C}$?

11.15. Characterize the maximal ideals in a product $\mathfrak{A} = \mathfrak{B} \times \mathfrak{C}$ of relation algebras.

11.16. Let M and N be the ideals in a product $\mathfrak{A} = \mathfrak{B} \times \mathfrak{C}$ of relation algebras that are defined by

$$M = B \times \{0\} \qquad \text{and} \qquad N = \{0\} \times C.$$

Prove that the quotient $\mathfrak{A}/M$ is isomorphic to $\mathfrak{C}$, and the quotient $\mathfrak{A}/N$ is isomorphic to $\mathfrak{B}$.

11.17. Formulate and prove a version of Lemma 11.8 that applies to infima.

11.18. Prove the associative law for direct products:

$$(\mathfrak{A} \times \mathfrak{B}) \times \mathfrak{C} \cong \mathfrak{A} \times (\mathfrak{B} \times \mathfrak{C}).$$

11.19. Prove the commutative law for direct products:

$$\mathfrak{A} \times \mathfrak{B} \cong \mathfrak{B} \times \mathfrak{A}.$$

11.20. Prove the identity law for direct products: if $\mathfrak{B}$ is a degenerate relation algebra, then

$$\mathfrak{A} \times \mathfrak{B} \cong \mathfrak{B} \times \mathfrak{A} \cong \mathfrak{A}.$$

11.21. Prove the distributive law for direct products over intersection: if $\mathfrak{B}$ and $\mathfrak{C}$ are both subalgebras of some relation algebra, then

$$\mathfrak{A} \times (\mathfrak{B} \cap \mathfrak{C}) = (\mathfrak{A} \times \mathfrak{B}) \cap (\mathfrak{A} \times \mathfrak{C}).$$

11.22. Prove the distributive law for direct products over join: if $\mathfrak{B}$ and $\mathfrak{C}$ are both subalgebras of some relation algebra $\mathfrak{D}$, then

$$\mathfrak{A} \times (\mathfrak{B} \vee \mathfrak{C}) = (\mathfrak{A} \times \mathfrak{B}) \vee (\mathfrak{A} \times \mathfrak{C}),$$

where the first occurrence of $\vee$ denotes the join operation on subalgebras of $\mathfrak{D}$, and the second denotes the join operation on subalgebras of $\mathfrak{A} \times \mathfrak{D}$.

11.23. Supply the missing details in the proof that the left and right projections on a product $\mathfrak{A} = \mathfrak{B} \times \mathfrak{C}$ are epimorphisms from $\mathfrak{A}$ to $\mathfrak{B}$ and to $\mathfrak{C}$ respectively.

11.24. For relation algebras $\mathfrak{A}$ and $\mathfrak{B}$, prove that $\mathfrak{A}$ is embeddable into the product $\mathfrak{A} \times \mathfrak{B}$ if and only if there is a homomorphism from $\mathfrak{A}$ into $\mathfrak{B}$.

11.25. Prove Corollary 11.10 directly, without using Theorem 11.9.

11.26. Prove that in a compactly generated, modular lattice with join and meet operations $\vee$ and $\wedge$ respectively, if $r \vee s$ and $r \wedge s$ are both compact elements, then r and s must be compact elements.

11.27. Fill in the missing details in the proof at the beginning of Section 11.4 that the direct product of two set relation algebras with disjoint base sets represents itself naturally as a set relation algebra.

11.28. Fill in the missing details in the proof that the function φ from the external product of two relation algebras to an internal product of the two algebras that is defined by $\varphi((s, t)) = s + t$ is an isomorphism.

11.29. Prove directly (without Theorem 11.15) that if $\mathfrak{A} = \mathfrak{B} \times \mathfrak{C}$, then $\mathfrak{A}$ is the internal product of the relativization of $\mathfrak{A}$ to $(1, 0)$ and the relativization of $\mathfrak{A}$ to $(0, 1)$.

11.30. Fill in the missing details in the proof that if relation algebras $\mathfrak{B}$ and $\mathfrak{C}$ are disjoint except for a common zero element, then the internal product $\mathfrak{B} \otimes \mathfrak{C}$ exists.

11.31. Fill in the missing details in the proof of Theorem 11.15.

11.32. Derive Theorem 11.15 as a consequence of Theorem 11.11 and the canonical isomorphism between external and internal products.

11.33. Formulate and prove a version of Lemma 11.7 for internal products.

11.34. Formulate and prove a version of Lemma 11.8 for internal products.

11.35. Formulate and prove a version of the associative law in Exercise 11.18 for internal products.

11.36. Formulate and prove a version of the commutative law in Exercise 11.19 for internal products.

11.37. Let $\mathfrak{A}$ be a relation algebra, and B the Boolean algebra of ideal elements in $\mathfrak{A}$. Prove that

$$\mathfrak{A} = \mathfrak{A}_1 \otimes \mathfrak{A}_2 \tag{1}$$

implies

$$B = B_1 \otimes B_2, \tag{2}$$

where B_1 and B_2 are the Boolean algebras of ideal elements in $\mathfrak{A}_1$ and $\mathfrak{A}_2$ respectively. (The decomposition in (2) is a Boolean decomposition of B.) Prove conversely that if (2) is any internal direct Boolean decomposition of B, then there is an internal direct decomposition of $\mathfrak{A}$ as in (1) such that B_1 and B_2 are the Boolean algebras of ideal elements in $\mathfrak{A}_1$ and $\mathfrak{A}_2$ respectively.

11.38. Prove that a relation algebra is directly indecomposable if and only if it is non-degenerate and is not isomorphic to the direct product of a system of two or more non-degenerate relation algebras.

11.39. Prove directly (without using Lemma 11.17) that the direct product of an arbitrary system of relation algebras is a relation algebra.

11.40. Prove Lemma 11.18.

11.41. Let $\mathfrak{B}$ and $\mathfrak{C}$ be relation algebras, put

$$\mathfrak{A}_0 = \mathfrak{B} \qquad \text{and} \qquad \mathfrak{A}_1 = \mathfrak{C},$$

and take $I = \{0, 1\}$. Prove that the products $\mathfrak{B} \times \mathfrak{C}$ and $\prod_{i \in I} \mathfrak{A}_i$ are not equal, but they are isomorphic. Thus, binary direct products may be identified with a special case of general direct products.

11.42. Prove Lemma 11.19.

11.43. Prove Corollary 11.20.

11.44. Prove Lemma 11.21.

11.45. Prove Lemma 11.22.

11.46. Prove Lemma 11.23.

11.47. Is the converse to Corollary 11.20 true? In other words, can every subalgebra of a direct product $\prod_i \mathfrak{A}_i$ of relation algebras be decomposed into a product of subalgebras of the factors $\mathfrak{A}_i$?

11.48. Under the hypotheses of Corollary 11.20, prove that $\prod_i \mathfrak{B}_i$ is a regular subalgebra of $\prod_i \mathfrak{A}_i$ if and only if $\mathfrak{B}_i$ is a regular subalgebra of $\mathfrak{A}_i$ for each index i.

11.49. Prove the following general associative law for direct products: if $(\mathfrak{A}_i : i \in I)$ is a system of relation algebras, and $(I_j : j \in J)$ a partition of the index set I, and if $\mathfrak{B}_j = \prod\{\mathfrak{A}_i : i \in I_j\}$ for each j in J, then

$$\prod\{\mathfrak{A}_i : i \in I\} \cong \prod\{\mathfrak{B}_j : j \in J\}.$$

11.50. Prove the following general commutative law for direct products: if $(\mathfrak{A}_i : i \in I)$ is a system of relation algebras, and π a permutation of the index set I, then

$$\prod\{\mathfrak{A}_i : i \in I\} \cong \prod\{\mathfrak{A}_{\pi(i)} : i \in I\}.$$

11.51. Prove the first law of exponentiation for direct powers: if $\mathfrak{A}$ is a relation algebra, and if I and J are disjoint sets, then

$$\mathfrak{A}^I \times \mathfrak{A}^J \cong \mathfrak{A}^{I \cup J}.$$

11.52. Prove the second law of exponentiation for direct powers: if $\mathfrak{A}$ is a relation algebra, then

$$(\mathfrak{A}^I)^J \cong \mathfrak{A}^{I \times J}.$$

11.53. Prove the third law of exponentiation for direct powers: if $\mathfrak{A}$ and $\mathfrak{B}$ are relation algebras, then

$$\mathfrak{A}^I \times \mathfrak{B}^I \cong (\mathfrak{A} \times \mathfrak{B})^I.$$

11.54. If $(\mathfrak{A}_i : i \in I)$ is a system of Boolean algebras with quasi-complete (or complete) operators, prove that the operations of the product algebra $\prod_i \mathfrak{A}_i$ are quasi-complete (or complete).

11.55. Fill in the missing details in the proof that the projection φ_i from $\mathfrak{A} = \prod_j \mathfrak{A}_j$ to $\mathfrak{A}_i$ is a complete epimorphism.

11.56. Fill in the missing details in the proof of Theorem 11.24.

11.57. Prove that the algebras in parts (i), (ii), and (iii) of Exercise 3.38 are respectively isomorphic to

$$\mathfrak{M}_1 \times \mathfrak{M}_1 \times \mathfrak{M}_1, \qquad \mathfrak{M}_1 \times \mathfrak{M}_2, \qquad \text{and} \qquad \mathfrak{M}_1 \times \mathfrak{M}_3.$$

11.58. For each i in an index set I, let $\mathfrak{A}_i$ be a set relation algebra with base set U_i and unit E_i. Prove that if the sets U_i are mutually disjoint, and if $E = \bigcup_i E_i$, then the direct product $\mathfrak{A} = \prod_i \mathfrak{A}_i$ is isomorphic to a subalgebra of $\mathfrak{Re}(E)$ via the mapping that assigns to each element R in $\mathfrak{A}$ the relation $\bigcup_i R_i$.

11.59. Prove that the operations of multiplication and relative addition in an internal product of relation algebras are performed componentwise, and that zero, one, and the diversity element in the internal product are respectively the componentwise sums of the zeros, ones, and diversity elements of the factor algebras.

11.60. Suppose $\mathfrak{A}$ is the internal product of a system of relation algebras $(\mathfrak{A}_i : i \in I)$, and $\gamma(v_0, v_1, \dots)$ is a term in the language of relation algebras. Prove that the operation defined by γ in $\mathfrak{A}$ is performed componentwise, that is to say, if $r, s, \dots$ are elements in $\mathfrak{A}$, then

$$\gamma^{\mathfrak{A}}(r, s, \dots) = \textstyle\sum_i \gamma^{\mathfrak{A}_i}(r_i, s_i, \dots).$$

11.61. Let $\mathfrak{B}$ be the external product, and $\mathfrak{A}$ the internal product, of a system of relation algebras $(\mathfrak{A}_i : i \in I)$. Fill in the missing details in the proof that the function φ defined by

$$\varphi(r) = \sum_i r_i$$

for each r in $\mathfrak{B}$ is an isomorphism from $\mathfrak{B}$ to $\mathfrak{A}$.

11.62. Fill in the missing details in the proof that two internal products of a system of relation algebras are always isomorphic via a mapping that is the identity function on the universes of the factor algebras.

11.63. Fill in the missing details in the proof that the internal product of a system of relation algebras exists if and only if the algebras in the system are disjoint except for a common zero element.

11.64. Give a direct proof of Corollary 11.36 that does not use the isomorphism between internal and external products.

11.65. Give a direct proof of Corollary 11.37 that does not use Lemma 11.22 and the isomorphism between internal and external products.

11.66. Give a direct proof of Corollary 11.38 that does not use Lemma 11.23 and the isomorphism between internal and external products.

11.67. Formulate and prove a version of Lemma 11.19 that applies to internal products. Give a direct proof that does not make use of the isomorphism between internal products and external products.

11.68. Formulate and prove a version of Corollary 11.20 that applies to internal products. Give a direct proof that does not make use of the isomorphism between internal products and external products.

11.69. Prove that an element in an internal product of a system of relation algebras is an equivalence element if and only if each component is an equivalence element in the corresponding factor algebra. Prove an analogous result for functions.

11.70. Fill in the missing details in the proof of Theorem 11.39.

11.71. Give an alternative proof of Theorem 11.39 by deriving it from Theorem 11.31, using the canonical isomorphism from an external to an internal product.

11.72. Define the notion of an internal product of a system of Boolean algebras. Prove that the product exists if and only if the algebras in the system are disjoint except for a common zero. Show further that the internal product is unique up to isomorphisms that are the identity on the factor algebras. Formulate and prove the analogue of Theorem 11.39 for Boolean algebras.

11.73. Let $(E_i : i \in I)$ be a system of mutually disjoint equivalence relations, and suppose E is the union of this system. Prove that $\mathfrak{Re}(E)$ is the internal product of the system $(\mathfrak{Re}(E_i) : i \in I)$.

11.74. Prove Theorem 11.43 directly, without using the Total Decomposition Theorem 11.41.

11.75. Can Exercise 11.37 be extended to infinite direct decompositions?

11.76. Suppose a relation algebra $\mathfrak{A}$ is the internal product of two different systems of relation algebras,

$$(\mathfrak{B}_i : i \in I) \qquad \text{and} \qquad (\mathfrak{C}_j : j \in J).$$

Prove that there is a system of relation algebras

$$(\mathfrak{D}_{ij} : i \in I \text{ and } j \in J)$$

with the property that $\mathfrak{A}$ is the internal product of this system, while $\mathfrak{B}_i$ is the internal product of the system $(\mathfrak{D}_{ij} : j \in J)$ for each i, and $\mathfrak{C}_j$ is the internal product of the system $(\mathfrak{D}_{ij} : i \in I)$ for each j. The system of algebras $\mathfrak{D}_{ij}$ is called a *common refinement* of the given systems of relation algebras. This exercise proves that the class of relation algebras has the *refinement property* with respect to direct decompositions, in the sense that two direct decompositions of a relation algebra always have a common refinement.

11.77. Use the refinement property in Exercise 11.76 to prove that if a relation algebra has a total decomposition, then that total decomposition is unique.

11.78. Prove that finite relation algebras obey the following *cancellation law for direct products*: if $\mathfrak{B} \times \mathfrak{C}$ and $\mathfrak{B} \times \mathfrak{D}$ are isomorphic, then $\mathfrak{C}$ and $\mathfrak{D}$ are isomorphic.

11.79. For finite relation algebras $\mathfrak{B}$ and $\mathfrak{C}$, if $\mathfrak{B} \times \mathfrak{B}$ and $\mathfrak{C} \times \mathfrak{C}$ are isomorphic, is it necessarily true that $\mathfrak{B}$ and $\mathfrak{C}$ are isomorphic? What if $\mathfrak{B}^n$ and $\mathfrak{C}^n$ are isomorphic for some positive integer $n > 2$?

11.80. Prove that a countable relation algebra with infinitely many ideal elements cannot have a total decomposition. Give an example of such a relation algebra.

11.81. Prove that a finite non-degenerate relation algebra $\mathfrak{A}$ is never isomorphic to its own square $\mathfrak{A} \times \mathfrak{A}$. Give an example to show that an infinite relation algebra may be isomorphic to its own square.

11.82. Prove that for each natural number n, the system $(I_\alpha : \alpha \in 2^n)$ of sets constructed in Section 11.12 is a partition of the given infinite set I.

11.83. Describe the elements $\hat{r}$ correlated in Section 11.12 with elements r in $\mathfrak{A}^{2^n}$ in the cases when $n = 2$ and $n = 3$.

11.84. Carry out the construction in Section 11.12 using a ternary tree (a tree in which there are three branches emanating from each node) of subsets of I. Be sure to explain how the ternary tree is constructed.

11.85. Carry out the construction in Section 11.12 using a tree of subsets of I that has a denumerably infinite number of branches emanating from each node. Be sure to explain how the tree is constructed.

11.86. Extend the theory of direct decompositions of relation algebras to discriminator varieties of Boolean algebras with operators (see Exercise 9.17).

11.87. Formulate and prove an external version of Theorem 11.49.

11.88. Prove that the internal amalgamation of a system of homomorphisms on a relation algebra $\mathfrak{A}$ is complete if and only if each homomorphism in the system is complete.

11.89. Let $\mathfrak{A}$ be a relation algebra, and φ_i a homomorphism from $\mathfrak{A}$ to a relation algebra $\mathfrak{B}_i$ for each i in some index set I. Prove directly, without using Lemma 11.50, that the function φ from $\mathfrak{A}$ into the product $\mathfrak{B} = \prod_i \mathfrak{B}_i$ defined by

$$\varphi(r) = (\varphi_i(r) : i \in I)$$

is a homomorphism from $\mathfrak{A}$ into $\mathfrak{B}$. Under what conditions is φ one-to-one? Onto? Complete?

11.90. Formulate and prove directly an external version of Theorem 11.51.

Chapter 12
Subdirect products

Every finite relation algebra can be represented as—that is to say, it is isomorphic to—a direct product of simple relation algebras, and this representation is unique up to permutations of the factors, by Corollary 11.45. But cardinality considerations imply that not every infinite relation algebra can be represented in this way. In more detail, if a totally decomposable relation algebra $\mathfrak{A}$ has an infinite Boolean algebra of ideal elements B, then B must be atomic, by Total Decomposition Theorem 11.41, and therefore B must have infinitely many atoms, since an atomic Boolean algebra with finitely many atoms is always finite. It follows that the total decomposition of $\mathfrak{A}$ must involve infinitely many simple factors, one for each atom in B, by Theorem 11.41. Now, the cardinality of a direct product of infinitely many simple relation algebras (each of which has, by definition, at least two elements) is always at least $2^{\aleph_0}$, the cardinality of the continuum of real numbers. Consequently, a countable relation algebra with an infinite Boolean algebra of ideal elements cannot be totally decomposable, that is to say, it cannot be represented as a direct product of simple relation algebras. For a concrete example of such a relation algebra, take any countably infinite Boolean relation algebra, such as the Boolean relation algebra of finite and cofinite subsets of the natural numbers.

In view of these considerations, it is natural to ask whether there are other product constructions, similar in spirit to direct products, that allow one to broaden the class of relation algebras that are representable as products of simple relation algebras. A natural place to look is the class of subalgebras of direct products. One such class of subalgebras—so-called weak direct products—plays an important role in the theory of groups with operators. This class is, however, not broad

S. Givant, *Introduction to Relation Algebras*,
DOI 10.1007/978-3-319-65235-1_12

enough. A more general class—so-called subdirect products—consists of those subalgebras of direct products that possess the additional property that each factor in the product is the homomorphic image of the subalgebra under the appropriate projection. As we shall see, this class is broad enough to capture all relation algebras in the sense that every relation algebra is isomorphic to a subdirect product of simple relation algebras.

12.1 Weak direct products

The weak direct product of a system of groups is the subgroup of the direct product consisting of those elements for which the ith coordinate is the group identity element in the ith factor group for all but finitely many indices i. A relation algebraic product $\mathfrak{A} = \prod_i \mathfrak{A}_i$ has a closely related subalgebra that is, however, more complicated to describe. It is helpful to introduce some terminology first. Suppose τ is a constant term in the language of relation algebras, that is to say, τ is a term built up from the constant symbol 1’ and the operation symbols of the language without using any variables. The value of τ in each factor algebra $\mathfrak{A}_i$ is an element—denote it by τ_i—that belongs to the minimal subalgebra of $\mathfrak{A}_i$. An element $r = (r_i : i \in I)$ in the direct product $\mathfrak{A}$ is said to be *constant almost everywhere* if there is a constant term τ such that $r_i = \tau_i$ for all but finitely many indices i. For example, if τ is the term 0’;0’, then r is an element in $\mathfrak{A}$ with the property that $r_i = (0’;0’)_i$ in $\mathfrak{A}_i$ for all but finitely many i. The first observation to make is that these elements form a subuniverse of $\mathfrak{A}$.

Lemma 12.1. *If $\mathfrak{A} = \prod_{i\in I} \mathfrak{A}_i$ is a product of relation algebras, then the set of elements in $\mathfrak{A}$ that are constant almost everywhere is a subuniverse of $\mathfrak{A}$.*

Proof. Let B be the set of elements in $\mathfrak{A}$ that are constant almost everywhere. Obviously, B contains the identity element r in $\mathfrak{A}$, because r is determined by the property that $r_i = \tau_i$ for every i, where τ is the constant symbol 1’ in the language of relation algebras.

The arguments showing that B is closed under the operations of $\mathfrak{A}$ are quite similar to one another, so we focus on the proof that B is closed under relative multiplication. Suppose

$$r = (r_i : i \in I) \qquad \text{and} \qquad s = (s_i : i \in I)$$

are elements in B, say ϱ and σ are constant terms in the language of relation algebras such that $r_i = \varrho_i$ for all i in some cofinite subset J of I, and $s_i = \sigma_i$ for all i in some cofinite subset K of I. The intersection $J \cap K$ is of course also a cofinite subset of I. Write $\tau = \varrho ; \sigma$ and observe that

$$r_i ; s_i = \varrho_i ; \sigma_i = (\varrho ; \sigma)_i = \tau_i$$

for all i in $J \cap K$. Since τ is a constant term, by the definition of such terms, and since

$$r ; s = (r_i ; s_i : i \in I),$$

by the definition of relative multiplication in $\mathfrak{A}$, it follows that the relative product $r ; s$ is constant almost everywhere and therefore belongs to B, by the definition of B. □

The *weak direct product* of a system $(\mathfrak{A}_i : i \in I)$ of relation algebras is defined to be the subalgebra $\mathfrak{B}$ of $\mathfrak{A} = \prod_i \mathfrak{A}_i$ whose universe is the set of elements in $\mathfrak{A}$ that are constant almost everywhere. This notion is well defined, by the preceding lemma. The algebras $\mathfrak{A}_i$ are called the *weak direct factors* of $\mathfrak{B}$. When no confusion can arise, we may simplify the terminology by speaking of the *weak product*— or the *weak external product*—of the system, and the *factors* of the weak product. Since equations are preserved under the formation of direct products and subalgebras, the weak direct product of a system of relation algebras is always a relation algebra.

There is also an internal version of the notion of a weak direct product. It is obtained by modifying the conditions in the definition of an internal product (Definition 11.34) in two ways. First of all, condition (ii) is weakened to read that the sum $\sum_i r_i$ exists in $\mathfrak{A}$ whenever r_i belongs to $\mathfrak{A}_i$ for each i, and the system of elements $(r_i : i \in I)$ is constant almost everywhere. Second, condition (iii) is modified to read that every element r in $\mathfrak{A}$ can be written in exactly one way as a sum $r = \sum r_i$ with r_i in $\mathfrak{A}_i$ for each i, and $(r_i : i \in I)$ constant almost everywhere. The other two conditions in the definition, namely conditions (i) and (iv), remain unchanged. The resulting algebra, if it exists, is called a *weak internal product* of the given system of algebras.

The questions that were raised in Section 11.9 concerning the existence and uniqueness of internal products can also be raised for weak internal products, and the answers are similar. First of all, there is a canonical isomorphism from the weak external product of a system of relation algebras to a weak internal product of the system, provided

the latter exists. In fact, the required isomorphism is just the restriction of the canonical isomorphism that exists from the external direct product to the internal direct product of the system. More precisely, it is the function that maps every system of elements $(r_i : i \in I)$ in the weak external product to the sum $\sum_i r_i$ in the weak internal product. From this observation it follows that two weak internal products of a system of relation algebras, if they exist, are isomorphic via a mapping that is the identity function on the universe of each of the factor algebras; the proof is completely analogous to the proof in the case of direct products. The existence of isomorphisms between different weak internal products of a given system of relation algebras justifies the practice of speaking of *the* weak internal product of the system. Finally, the internal product of a system of relation algebras exists if and only if the algebras in the system are disjoint except for a common zero. In what follows, we always assume tacitly that any system of relation algebras for which the internal or weak internal product is being formed has this disjointness property. The following is an internal version of the *Weak Product Decomposition Theorem*.

Theorem 12.2. *A relation algebra $\mathfrak{A}$ is the weak internal product of a system of relation algebras $(\mathfrak{A}_i : i \in I)$ if and only if there is a system $(u_i : i \in I)$ of ideal elements in $\mathfrak{A}$ partitioning the unit such that $\mathfrak{A}(u_i) = \mathfrak{A}_i$ for each i, and the set $\bigcup_i A_i$ generates $\mathfrak{A}$.*

Proof. Assume there exists a system

$$(u_i : i \in I) \tag{1}$$

of ideal elements in $\mathfrak{A}$ with the following properties. First, the system partitions the unit of $\mathfrak{A}$ in the sense that the elements in the system are mutually disjoint and sum to 1. Second,

$$\mathfrak{A}(u_i) = \mathfrak{A}_i \tag{2}$$

for each index i. Third, the set

$$X = \bigcup_i A_i \tag{3}$$

generates $\mathfrak{A}$. In order to prove that $\mathfrak{A}$ is the weak internal product of the given system of relation algebras, it must be shown that the four conditions (i)–(iv) in the definition of a weak internal product (see the beginning of the section) are satisfied.

The proofs that conditions (i) and (iv) hold in $\mathfrak{A}$ are the same as in the proof of the internal version of the Product Decomposition Theorem 11.39. In fact, only (2) and the partition properties of the system in (1) are used in the proof of that theorem to verify these two conditions; in particular, the supremum property plays no role in that part of the proof.

Before proving that condition (ii) holds, we make a preliminary observation. If τ is a constant term in the language of relation algebras, and if τ_i denotes the value of τ in the factor algebra $\mathfrak{A}_i$, then the value of τ in $\mathfrak{A}$ is just the sum $\sum_i \tau_i$ in $\mathfrak{A}$, in symbols,

$$\tau^{\mathfrak{A}} = \textstyle\sum_i \tau_i. \tag{4}$$

The proof of (4) proceeds by induction on terms and uses the validity of condition (iv) in $\mathfrak{A}$, which has already been established. The constant terms are the terms obtained from the individual constant symbol 1' by repeated applications of the operation symbols of the language of relation algebras. The observation is certainly true when τ is the constant symbol 1', by the clause in condition (iv) regarding the identity element. If τ has the form $\tau = \varrho\,;\sigma$ for some constant terms ϱ and σ, and if the observation is true for ϱ and σ, then

$$\rho^{\mathfrak{A}} = \textstyle\sum_i \rho_i \qquad \text{and} \qquad \sigma^{\mathfrak{A}} = \textstyle\sum_i \sigma_i, \tag{5}$$

and therefore

$$\begin{aligned}\tau^{\mathfrak{A}} = (\rho\,;\sigma)^{\mathfrak{A}} = \rho^{\mathfrak{A}}\,;\sigma^{\mathfrak{A}} = (\textstyle\sum_i \rho_i)\,;(\textstyle\sum_i \sigma_i)& \\ = \textstyle\sum_i(\rho_i\,;\sigma_i) = \textstyle\sum_i(\rho\,;\sigma)_i = \textstyle\sum_i \tau_i&.\end{aligned}$$

The first and last equalities use the assumption about the form of τ, the second and fifth use the inductive definition of the value of a term in an algebra, the third uses the induction hypothesis (5), and the fourth uses the clause in condition (iv) regarding relative multiplication. Thus, (4) holds in this case. The other cases in the proof of (4) are handled in a similar fashion.

To verify condition (ii) in $\mathfrak{A}$, consider a system of elements

$$(r_i : i \in I) \tag{6}$$

that is constant almost everywhere and such that r_i is in $\mathfrak{A}_i$ for each index i. It is to be shown that the sum $\sum_i r_i$ exists in $\mathfrak{A}$. With an eye

to a later part of the proof, we shall prove a bit more, namely that the validity of condition (iv) in $\mathfrak{A}$ (which was established above) implies by itself—without further hypotheses (and in particular without using the hypothesis that the set X defined in (3) generates $\mathfrak{A}$)—that the sum $\sum_i r_i$ is in fact an element in the subalgebra of $\mathfrak{A}$ generated by X.

The assumption on the system in (6) implies the existence of a constant term τ in the language of relation algebras and a cofinite subset J of I such that $r_i = \tau_i$ for all i in J. The value of τ in $\mathfrak{A}$ is an element in the minimal subalgebra of $\mathfrak{A}$, since τ is a constant term; so this value is generated by the empty set. Consequently, the sum $\sum_i \tau_i$ is generated by the empty set, and hence belongs to the subalgebra generated by X, by the preliminary observation in (4). The systems of elements $(s_i : i \in I)$ and $(t_i : i \in I)$ defined by

$$s_i = \begin{cases} 0 & \text{if} \quad i \in J, \\ r_i & \text{if} \quad i \in I \sim J, \end{cases} \qquad \text{and} \qquad t_i = \begin{cases} 0 & \text{if} \quad i \in J\,, \\ \tau_i & \text{if} \quad i \in I \sim J, \end{cases}$$

are zero almost everywhere, and the finitely many non-zero components of each system belong to the set X, by (3), so the (essentially finite) sums $\sum_i s_i$ and $\sum_i t_i$ also belong to the subalgebra generated by X. It follows that the Boolean combination

$$((\textstyle\sum_i \tau_i) - (\sum_i t_i)) + (\sum_i s_i)$$

of these three sums belongs to the subalgebra generated by X. Condition (iv) implies that

$$((\textstyle\sum_i \tau_i) - (\sum_i t_i)) + (\sum_i s_i) = \sum_i ((\tau_i - t_i) + s_i).$$

If i is in J, then

$$(\tau_i - t_i) + s_i = (\tau_i - 0) + 0 = \tau_i = r_i,$$

and if i is in $I \sim J$, then

$$(\tau_i - t_i) + s_i = (\tau_i - \tau_i) + r_i = 0 + r_i = r_i.$$

Combine these observations to conclude that

$$((\textstyle\sum_i \tau_i) - (\sum_i t_i)) + (\sum_i s_i) = \sum_i r_i$$

and therefore that $\sum_i r_i$ belongs to the subalgebra generated by X.

Turn now to the verification of condition (iii). In order to prove that every element in $\mathfrak{A}$ can be written in at least one way as the sum of a system of elements that is constant almost everywhere, consider the set B of elements in $\mathfrak{A}$ that can be so written. It is to be shown that $A = B$. Observe that B contains the identity element and is closed under the operations of $\mathfrak{A}$. The proof of this observation uses the validity of condition (iv) in $\mathfrak{A}$ and is similar to the proof of Lemma 12.1; the details are left to the reader. The observation implies that B is a subuniverse of $\mathfrak{A}$. Every element r in $\mathfrak{A}_i$ is the sum of a system of elements that is constant almost everywhere, namely the system of elements $(r_j : j \in I)$ defined by

$$r_j = \begin{cases} r & \text{if} \quad j = i, \\ 0 & \text{if} \quad j \neq i. \end{cases}$$

Consequently, the universe of $\mathfrak{A}_i$ is included in the set B. This is true for each index i, so the set X must be included in B, by (3). It follows that the subuniverse of $\mathfrak{A}$ generated by X must also be included in B, because B is a subuniverse of $\mathfrak{A}$. The subuniverse of $\mathfrak{A}$ generated by X is the set A, by assumption, so $A = B$, as required.

The argument that every element in $\mathfrak{A}$ can be written in at most one way as the sum of a system of elements that is constant almost everywhere is identical to the argument of the analogous result in the proof of Theorem 11.39. Indeed, the argument presented there uses only (2) and the assumption that the elements in (1) are mutually disjoint. Conclusion: conditions (i)–(iv) hold in $\mathfrak{A}$, so $\mathfrak{A}$ is the weak internal product of the given system of relation algebras.

To establish the reverse direction of the theorem, assume that $\mathfrak{A}$ is the weak internal product of the given system of relation algebras. Thus, conditions (i)–(iv) in the definition of a weak internal product hold in $\mathfrak{A}$, and it is to be shown that there is a system (1) of ideal elements partitioning the unit and satisfying (2) such that the set X defined in (3) generates $\mathfrak{A}$.

As in the proof of Theorem 11.39, let u_i be the unit of $\mathfrak{A}_i$ for each index i. The arguments in the second part of the proof of Theorem 11.39, showing that $\sum_i u_i = 1$, that u_i and u_j are disjoint for $i \neq j$, and that each element u_i is an ideal element, remain valid in the present context. Indeed, those arguments involve only conditions (i) and (iv) from the definition of an internal product (Definition 11.34)—conditions that remain unchanged in the definition of a weak internal product—and

use only systems of elements that are constant almost everywhere. The argument in the proof of Theorem 11.39 that (2) holds does make use of condition (iii) for internal products, in addition to conditions (i) and (iv), but the application of condition (iii) in that proof may be replaced in the present context by the version of condition (iii) that is applicable to weak internal product. The remaining details of the verification of (2) remain unchanged. Conclusion: the system (1) of units of the factor algebras $\mathfrak{A}_i$ consists of ideal elements, partitions the unit of $\mathfrak{A}$, and satisfies (2).

It remains to prove that the set X defined in (3) generates $\mathfrak{A}$. As was argued above, the sum of every system of elements that is constant almost everywhere is generated by X. Since $\mathfrak{A}$ consists of precisely such sums, by conditions (ii) and (iii) in the definition of a weak internal product, it follows that X generates $\mathfrak{A}$. □

Corollary 12.3. *The weak internal product of a system of relation algebras is just the subalgebra of the internal product that is generated by the union of the universes of the factor algebras.*

Proof. Let $\mathfrak{A}$ be the internal product of a system $(\mathfrak{A}_i : i \in I)$ of relation algebras, and let $\mathfrak{B}$ be the subalgebra of $\mathfrak{A}$ generated by the set

$$X = \bigcup_i A_i .$$

The system of units

$$(u_i : i \in I) \tag{1}$$

of the individual factor algebras is a partition of the unit in $\mathfrak{A}$, and $\mathfrak{A}(u_i) = \mathfrak{A}_i$ for each i, by the internal version of the Product Decomposition Theorem 11.39. The algebra $\mathfrak{B}$ is a subalgebra of $\mathfrak{A}$ that includes the universe of $\mathfrak{A}_i$ for each i, by assumption, so the system in (1) remains a partition of the unit in $\mathfrak{B}$, and $\mathfrak{B}(u_i) = \mathfrak{A}_i$ for each i. Apply Theorem 12.2 to conclude that $\mathfrak{B}$ is the weak internal product of the given system of relation algebras. □

The preceding theorem and corollary are examples of results about weak products for which the internal versions seem to have much more natural formulations than the external versions.

Several of the preservation theorems for direct products have versions that apply to weak direct products. Here are two examples.

Lemma 12.4. *The ideal elements in the weak internal product of a system of relation algebras are just the sums of systems of ideal elements that are constant almost everywhere. In particular, the ideal element atoms in the internal product are just the ideal element atoms in the factor algebras.*

In other words, r is an ideal element in the weak internal product of a system of relation algebras $(\mathfrak{A}_i : i \in I)$ if and only if $r = \sum_i r_i$ for some system of elements $(r_i : i \in I)$ with two properties: first, there is a constant term τ denoting an ideal element in each factor algebra $\mathfrak{A}_i$ such that $r_i = \tau_i$ for all indices i in some cofinite subset J of I; and second, r_i is an ideal element in $\mathfrak{A}_i$ for each i in $I \sim J$.

Lemma 12.5. *The atoms in the weak internal product of a system of relation algebras are just the atoms in the factor algebras. The product is atomic if and only if each factor algebra is atomic.*

Weak internal products of infinite systems of non-degenerate relation algebras are incomplete, even when the factor algebras are all complete, because the supremum property fails. For that reason, an analogue of Corollary 11.38 for weak internal products fails to be true.

12.2 Ample internal products

Condition (ii) in the definition of an internal product (Definition 11.34) requires that every sum of the form $\sum_i r_i$, with r_i in $\mathfrak{A}_i$ for each i, exist in $\mathfrak{A}$, while condition (iii) requires that every element in $\mathfrak{A}$ be writable in exactly one way as such a sum. The notion of a weak internal product is obtained by first weakening condition (ii) to require only that sums of the form $\sum_i r_i$, with r_i in $\mathfrak{A}_i$ for each i, exist in $\mathfrak{A}$ when the system $(r_i : i \in I)$ is constant almost everywhere, and then strengthening condition (iii) in a corresponding way to require that every element in $\mathfrak{A}$ be writable in a unique way as the sum of such an almost constant system of elements. It is natural to ask what algebras are obtained if the original condition (ii) is deleted altogether, and the original condition (iii) is left intact.

Call a relation algebra $\mathfrak{A}$ an *ample internal product* of a system of relation algebras $(\mathfrak{A}_i : i \in I)$ if conditions (i), (iii), and (iv) of Definition 11.34 hold. As in the case of internal and weak internal products, ample internal products can only exist if the given system of

relation algebras is disjoint except for a common zero element. In what follows, we tacitly assume that this is always the case. In contrast to the situation for internal and weak internal products, ample internal products are not uniquely determined. In fact, both internal and weak internal products are instances of ample internal products. What is true is that ample internal products are subalgebras of the internal product that include the weak internal product.

Lemma 12.6. *A relation algebra $\mathfrak{A}$ is an ample internal product of a system of relation algebras if and only if $\mathfrak{A}$ is (up to isomorphism) a subalgebra of the internal product of the system and $\mathfrak{A}$ includes the weak internal product of the system as a subalgebra.*

Proof. Let $\mathfrak{B}$ be the internal product of a system of relation algebras

$$(\mathfrak{A}_i : i \in I), \tag{1}$$

and let $\mathfrak{C}$ be the subalgebra of $\mathfrak{B}$ generated by the set

$$X = \textstyle\bigcup_i A_i .$$

Notice that $\mathfrak{C}$ is the weak internal product of the system in (1), by Corollary 12.3.

Assume first that $\mathfrak{A}$ is an ample internal product of (1). Each element r in $\mathfrak{A}$ has the form $\sum_i r_i$ for a uniquely determined system of elements $(r_i : i \in I)$ with the property that r_i is in $\mathfrak{A}_i$ for each i, by condition (iii) in the definition of an ample internal product. A corresponding uniquely determined sum $\bar{r} = \sum_i r_i$ must exist in $\mathfrak{B}$, by conditions (ii) and (iii) in Definition 11.34. Identify each element r in $\mathfrak{A}$ with the corresponding element $\bar{r}$ in $\mathfrak{B}$. Under this identification, the validity of condition (iv) in $\mathfrak{A}$ and $\mathfrak{B}$ implies that $\mathfrak{A}$ is a subalgebra of $\mathfrak{B}$. In more detail, if elements

$$r = \textstyle\sum_i r_i \qquad \text{and} \qquad s = \textstyle\sum_i s_i$$

in $\mathfrak{A}$ are respectively identified with elements $\bar{r}$ and $\bar{s}$ in $\mathfrak{B}$, then

$$r \mathbin{;} s = \textstyle\sum_i r_i \mathbin{;} s_i \qquad \text{and} \qquad \bar{r} \mathbin{;} \bar{s} = \textstyle\sum_i r_i \mathbin{;} s_i$$

in $\mathfrak{A}$ and in $\mathfrak{B}$ respectively, by the validity of condition (iv) in $\mathfrak{A}$ and in $\mathfrak{B}$. Consequently, the relative product $r \mathbin{;} s$ in $\mathfrak{A}$ is identified with the relative product $\bar{r} \mathbin{;} \bar{s}$ in $\mathfrak{B}$, that is to say, $\overline{r \mathbin{;} s} = \bar{r} \mathbin{;} \bar{s}$, so the identification of elements in $\mathfrak{A}$ with elements in $\mathfrak{B}$ preserves the operation of

relative multiplication. Similar arguments show that the identification preserves the remaining operations of $\mathfrak{A}$. Thus, under the identification, $\mathfrak{A}$ becomes a subalgebra of $\mathfrak{B}$. (More precisely, the identification is an embedding of $\mathfrak{A}$ into $\mathfrak{B}$.) Furthermore, the universe of each factor algebra $\mathfrak{A}_i$ is included in $\mathfrak{A}$, by condition (i) in the definition of an ample internal product, so the set X must be included in $\mathfrak{A}$, and therefore the weak internal product $\mathfrak{C}$ (which is generated by X) must be a subalgebra of $\mathfrak{A}$.

To establish the reverse implication in the lemma, assume that $\mathfrak{C}$ is a subalgebra of $\mathfrak{A}$, and $\mathfrak{A}$ a subalgebra of $\mathfrak{B}$. The universe of every factor algebra $\mathfrak{A}_i$ is included in $\mathfrak{C}$, so these universes must also be included in $\mathfrak{A}$. Thus, condition (i) holds in $\mathfrak{A}$. Conditions (iii) and (iv) from Definition 11.34 hold in $\mathfrak{B}$, by the assumption that $\mathfrak{B}$ is the internal product of (1), so these conditions (because of their universal nature) hold in all subalgebras of $\mathfrak{B}$ that include the set X. In particular, they hold in $\mathfrak{A}$. Thus, $\mathfrak{A}$ is an ample internal product of the system in (1). □

The decomposition theorems for internal and weak internal products (Theorems 11.39 and 12.2) have a very natural analogue for ample internal products.

Theorem 12.7. *A relation algebra $\mathfrak{A}$ is an ample internal product of a system of relation algebras $(\mathfrak{A}_i : i \in I)$ if and only if there is a system $(u_i : i \in I)$ of ideal elements in $\mathfrak{A}$ partitioning the unit such that $\mathfrak{A}(u_i) = \mathfrak{A}_i$ for each i.*

The proof of this theorem is very similar to the proof of Theorem 11.39. In fact, it can be obtained from the proof of the latter theorem by omitting those portions of the proof that pertain to condition (ii) and the supremum property. The details are left as an exercise.

12.3 Subdirect products

It is clear from the discussion at the beginning of the chapter that not every relation algebra can be represented as a direct product of simple relation algebras, but a weaker result is true: every relation algebra is a subdirect product of simple relation algebras.

An algebra $\mathfrak{A}$ is said to be a *subdirect product* of a system of relation algebras $(\mathfrak{A}_i : i \in I)$ if $\mathfrak{A}$ is a subalgebra of the direct product of the

system, and if, for each index i, the ith projection from the direct product to the factor algebra $\mathfrak{A}_i$ maps $\mathfrak{A}$ onto $\mathfrak{A}_i$. The algebras $\mathfrak{A}_i$ are called *subdirect factors* of $\mathfrak{A}$. One obtains external and internal versions of these notions according to whether the direct product one uses is the external or the internal product of the system of relation algebras.

An isomorphism from $\mathfrak{A}$ to a subdirect product of a system of relation algebras is called a *subdirect representation* of $\mathfrak{A}$. In other words, a mapping φ is a subdirect representation of $\mathfrak{A}$ if φ is an embedding of $\mathfrak{A}$ into the direct product of some system $(\mathfrak{A}_i : i \in I)$ of relation algebras, and if, for each index i, the ith projection ψ_i from the direct product of the system onto $\mathfrak{A}_i$ maps the image of $\mathfrak{A}$ under φ onto $\mathfrak{A}_i$. This last condition is clearly equivalent to the condition that the composition $\psi_i \circ \varphi$ maps $\mathfrak{A}$ onto $\mathfrak{A}_i$ for each index i.

The direct product of a system of relation algebras is an obvious example of a subdirect product. Another example is the weak direct product of the system. More generally, any subalgebra of the direct product that includes the weak direct product as a subalgebra—that is to say, any ample direct product of the system—is a subdirect product of the system.

For a different kind of example of a subdirect product, consider an arbitrary relation algebra $\mathfrak{B}$ and an arbitrary non-empty index set I. The set of constant systems in the Ith power $\mathfrak{B}^I$—that is to say, the set of elements of the form $(r, r, r, \dots)$ for r in $\mathfrak{B}$—contains the identity element of $\mathfrak{B}^I$, by the definition of this element, and is closed under the operations of $\mathfrak{B}^I$, because these operations are performed coordinatewise. Consequently, this set is the universe of a subalgebra $\mathfrak{A}$ of $\mathfrak{B}^I$. For each index i, the ith projection of $\mathfrak{B}^I$ onto the factor algebra $\mathfrak{B}$ maps each element $(r, r, r, \dots)$ in $\mathfrak{A}$ to the element r, and therefore maps $\mathfrak{A}$ onto $\mathfrak{B}$. It follows that the subalgebra $\mathfrak{A}$ is a subdirect product of the system of relation algebras $(\mathfrak{A}_i : i \in I)$ with $\mathfrak{A}_i = \mathfrak{B}$ for each i.

For each index i in I, let φ_i be the identity automorphism of $\mathfrak{B}$. The external amalgamation φ of the system $(\varphi_i : i \in I)$ is the homomorphism from $\mathfrak{B}$ into $\mathfrak{B}^I$ that is defined by

$$\varphi(r) = (\varphi_i(r) : i \in I) = (r, r, r, \dots)$$

(see Section 11.13), and this homomorphism is obviously one-to-one. It is called the *diagonal embedding* of $\mathfrak{B}$ into $\mathfrak{B}^I$, and it clearly maps $\mathfrak{B}$ isomorphically to the subalgebra $\mathfrak{A}$ of $\mathfrak{B}^I$ defined in the preceding paragraph. Thus, φ is a subdirect representation of $\mathfrak{B}$. The identity

automorphism of $\mathfrak{B}$ is of course also a subdirect representation of $\mathfrak{B}$. Consequently, subdirect representations of a relation algebra are very far from being uniquely determined, even when the algebra in question is simple.

The main goal of this section is to prove that every relation algebra is isomorphic to a subdirect product of simple relation algebras. The ideas seem easiest to express using external products, so in this section all direct products considered will be external ones. We begin with a general *Subdirect Decomposition Theorem*.

Theorem 12.8. *A relation algebra $\mathfrak{A}$ is isomorphic to a subdirect product of a system $(\mathfrak{A}_i : i \in I)$ of relation algebras if and only if there is a system $(M_i : i \in I)$ of ideals in $\mathfrak{A}$ such that $\bigcap_i M_i = \{0\}$ and $\mathfrak{A}/M_i$ is isomorphic to $\mathfrak{A}_i$ for each i.*

Proof. Suppose first that $(M_i : i \in I)$ is a system of ideals in $\mathfrak{A}$ possessing the requisite properties. For each index i, take φ_i to be the quotient homomorphism from $\mathfrak{A}$ onto $\mathfrak{A}/M_i$. The amalgamation φ of the system of these quotient homomorphisms is the embedding of $\mathfrak{A}$ into the external product of the system

$$(\mathfrak{A}/M_i : i \in I) \tag{1}$$

that is defined by

$$\varphi(r) = (\varphi_i(r) : i \in I) = (r/M_i : i \in I)$$

for each r in $\mathfrak{A}$, by the external version of Lemma 11.50. If ψ_i is the projection of this product onto the factor $\mathfrak{A}/M_i$, then φ is also the amalgamation of the system of compositions $(\psi_i \circ \varphi : i \in I)$, and consequently $\varphi_i = \psi_i \circ \varphi$ for each i, by the Second Homomorphism Decomposition Theorem 11.51. Since the mapping φ_i is onto, the composition $\psi_i \circ \varphi$ must be onto. Consequently, φ is an isomorphism from $\mathfrak{A}$ to a subdirect product of the system in (1). The quotient $\mathfrak{A}/M_i$ is isomorphic to $\mathfrak{A}_i$ for each i, by assumption, so the product of the system in (1) must be isomorphic to the product of the system of algebras

$$(\mathfrak{A}_i : i \in I) \tag{2}$$

via the product isomorphism ϑ, by Lemma 11.21. The composition $\vartheta \circ \varphi$ is clearly an isomorphism from $\mathfrak{A}$ to a subdirect product of the system in (2).

To establish the reverse direction of the theorem, assume that φ is an isomorphism from $\mathfrak{A}$ to a subdirect product of the system in (2). Let ψ_i be the projection from the direct product of the system in (2) to the factor $\mathfrak{A}_i$. The composition $\psi_i \circ \varphi$ must map $\mathfrak{A}$ onto $\mathfrak{A}_i$, by the remarks at the beginning of the section concerning subdirect representations, and φ must be the amalgamation of the system of these compositions, by Theorem 11.51. Take M_i to be the ideal that is the kernel of $\psi_i \circ \varphi$. The kernel of φ is the trivial ideal because φ is one-to-one, so the intersection of the system of ideals $(M_i : i \in I)$ is the trivial ideal, by Lemma 11.50. Furthermore, the quotient $\mathfrak{A}/M_i$ is isomorphic to $\mathfrak{A}_i$, by the First Isomorphism Theorem 8.39. □

Of the various subdirect decompositions that a relation algebra may possess, the most important are those in which the factors of the decomposition are irreducible in some sense. A relation algebra $\mathfrak{A}$ is said to be *subdirectly irreducible* if it is non-degenerate and satisfies the following condition: whenever φ is a subdirect representation of $\mathfrak{A}$, one of the projections of φ is already an isomorphism. In other words, $\mathfrak{A}$ is isomorphic, via a projection of φ, to one of the factors of the product into which it is being embedded. This notion also has an intrinsic lattice-theoretic characterization.

Lemma 12.9. *The following conditions on a relation algebra* $\mathfrak{A}$ *are equivalent.*

(i) $\mathfrak{A}$ *is subdirectly irreducible.*
(ii) $\mathfrak{A}$ *has a smallest non-trivial ideal.*
(iii) *Every set of non-zero ideal elements in* $\mathfrak{A}$ *has a non-zero lower bound.*
(iv) $\mathfrak{A}$ *has a smallest non-zero ideal element.*

Proof. We begin with the proof of the implication from (ii) to (i). Suppose $\mathfrak{A}$ has a smallest non-trivial ideal. Certainly, $\mathfrak{A}$ is non-degenerate, since degenerate relation algebras cannot have non-trivial ideals. Consider now any isomorphism φ from $\mathfrak{A}$ to a subdirect product of a system of relation algebras $(\mathfrak{A}_i : i \in I)$. For each index i, let ψ_i be the projection from the product of this system onto $\mathfrak{A}_i$. The composition $\psi_i \circ \varphi$ is a homomorphism from $\mathfrak{A}$ onto $\mathfrak{A}_i$ for each i, by the assumption that φ is a subdirect representation of $\mathfrak{A}$. Write M_i for the kernel of this homomorphism. The intersection $\bigcap_i M_i$ is the trivial ideal, by Theorem 12.8 (and its proof), so condition (ii) implies that at least one of the ideals M_i must be trivial; otherwise, the intersection of

the ideals would include the smallest non-trivial ideal. If M_i is trivial, then $\psi_i \circ \varphi$ is one-to-one and therefore an isomorphism from $\mathfrak{A}$ to $\mathfrak{A}_i$. This is true for any subdirect representation φ of $\mathfrak{A}$, so $\mathfrak{A}$ is subdirectly irreducible.

Turn next to the implication from (i) to (iii). Assume that $\mathfrak{A}$ is subdirectly irreducible, and consider a set

$$\{r_i : i \in I\} \tag{1}$$

of non-zero ideal elements in $\mathfrak{A}$. It is to be shown that this set has a non-zero lower bound. For each index i, take $\mathfrak{A}_i$ to be the quotient of $\mathfrak{A}$ modulo the principal ideal (r_i), and let φ_i be the quotient homomorphism from $\mathfrak{A}$ onto $\mathfrak{A}_i$. Notice that φ_i is not one-to-one, because its kernel (r_i) is not the trivial ideal. The function φ that is the amalgamation of the system of these quotient homomorphisms is a homomorphism from $\mathfrak{A}$ into the direct product $\mathfrak{B}$ of the system of quotient algebras, by Lemma 11.50. The mapping φ is also the amalgamation of the projections $\psi_i \circ \varphi$, and

$$\psi_i \circ \varphi = \varphi_i \tag{2}$$

for each i, by Theorem 11.51. Since each quotient homomorphism φ_i maps $\mathfrak{A}$ onto $\mathfrak{A}_i$ and is not one-to-one, it follows from (2) that each projection $\psi_i \circ \varphi$ maps $\mathfrak{A}$ onto $\mathfrak{A}_i$ and is not one-to-one. This observation implies that φ cannot be one-to-one; for if it were, then it would be a subdirect representation of $\mathfrak{A}$ with the property that none of its projections is an isomorphism from $\mathfrak{A}$ onto the corresponding factor algebra, in contradiction to the assumption that $\mathfrak{A}$ is subdirectly irreducible. Since φ is not one-to-one, it must map some non-zero element s in $\mathfrak{A}$ to the zero element of the product $\mathfrak{B}$. Consequently, φ_i must map s to the zero element of $\mathfrak{A}_i$ for each index i, because φ is the amalgamation of the mappings φ_i. This implies that s belongs to the kernel of the quotient homomorphism φ_i—that is to say, s belongs to the ideal (r_i) and is therefore below the ideal element r_i—for each index i. Conclusion: s is a non-zero lower bound of the set in (1).

To establish the implication from (iii) to (iv), assume (iii) holds and let (1) be the set of all non-zero ideal elements in $\mathfrak{A}$. This set has a non-zero lower bound s, by (iii). For each index i, we have $0 < s \leq r_i$ and therefore

$$0 < s \leq 1 \,;\, s \,;\, 1 \leq 1 \,;\, r_i \,;\, 1 = r_i ,$$

by Lemma 4.5(iii) and its first dual, the monotony law for relative multiplication, the assumption that r_i is an ideal element, and the definition of an ideal element. Thus, $1 ; s ; 1$ is also a non-zero lower bound for the set in (1), and it is an ideal element, by Lemma 5.38(ii). Since (1) consists of all of the non-zero ideal elements in $\mathfrak{A}$, it follows that $1 ; s ; 1$ must the smallest non-zero ideal element in $\mathfrak{A}$.

Turn finally to the implication from (iv) to (ii). Assume that (iv) holds, say s is the smallest non-zero ideal element in $\mathfrak{A}$. Consider an arbitrary non-trivial ideal M in $\mathfrak{A}$, and let r be an arbitrary non-zero element in M. The ideal element $1 ; r ; 1$ also belongs to M, by Definition 8.7(iv); moreover, this ideal element is non-zero, because it is above r, by Lemma 4.5(iii) and its first dual. The element s is, by assumption, the smallest non-zero ideal element, so it is below $1 ; r ; 1$ and therefore it also belongs to M, by Lemma 8.8(v). Consequently, the principal ideal (s) is included in M, by Lemma 8.8(v). Conclusion: (s) is the smallest non-trivial ideal in $\mathfrak{A}$. □

The reader may be bothered by one point in the preceding lemma. Why is a relation algebra $\mathfrak{A}$ that satisfies condition (iii) necessarily non-degenerate? The reason is that the empty set of ideal elements is allowed in the condition. Since this set is required by the condition to have a non-zero lower bound, $\mathfrak{A}$ cannot be degenerate. An equivalent formulation of condition (iii) is that for any system of ideal elements $(r_i : i \in I)$ in $\mathfrak{A}$,

$$\prod_i r_i = 0 \qquad \text{implies} \qquad r_i = 0$$

for some i. This formulation is used in Section 9.3.

The preceding lemma immediately implies the conclusion already mentioned in Theorem 9.12 that a subdirectly irreducible relation algebra is necessarily simple. Indeed, if a non-degenerate relation algebra $\mathfrak{A}$ is not simple, then there must be an ideal element r in $\mathfrak{A}$ that is different from both 0 and 1, by Lemma 9.1. The system consisting of the two non-zero ideal elements r and $-r$ has zero as its product, so $\mathfrak{A}$ cannot be subdirectly irreducible, by Lemma 12.9.

An algebra is called *semi-simple* if it is isomorphic to a subdirect product of simple algebras. The next theorem says that every relation algebra is semi-simple, so we shall call it the *Semi-simplicity Theorem*.

Theorem 12.10. *Every relation algebra is isomorphic to a subdirect product of simple relation algebras.*

Proof. Consider an arbitrary relation algebra $\mathfrak{A}$, and take I to be the set of non-zero elements in $\mathfrak{A}$. For each index i—that is to say, for each non-zero element i in $\mathfrak{A}$—let M_i be a maximal ideal in $\mathfrak{A}$ that does not contain i. Such an ideal exists by the Maximal Ideal Theorem 8.31 (with the trivial ideal in place of M). Observe that the quotients $\mathfrak{A}/M_i$ are all simple relation algebras, by Lemma 9.6.

Take φ_i to be the quotient homomorphism from $\mathfrak{A}$ onto $\mathfrak{A}/M_i$, and note that M_i is the kernel of φ_i. The intersection of the system of ideals $(M_i : i \in I)$ is the trivial ideal, since each non-zero element i in $\mathfrak{A}$ is omitted by one of the ideals in the system, namely the ideal M_i. The amalgamation φ of the system of quotient homomorphisms is the function on $\mathfrak{A}$ defined by

$$\varphi(r) = (\varphi_i(r) : i \in I) = (r/M_i : i \in I)$$

for r in $\mathfrak{A}$, and it is an embedding from $\mathfrak{A}$ into the product

$$\mathfrak{B} = \prod_i \mathfrak{A}/M_i,$$

by the external version of Lemma 11.50.

The embedding φ is the amalgamation of the system of its projections, and this representation of φ as an amalgamation is unique, by the external version of the Second Homomorphism Decomposition Theorem 11.51. Thus, if ψ_i is the projection of the product $\mathfrak{B}$ onto the factor $\mathfrak{A}/M_i$, then $\psi_i \circ \varphi = \varphi_i$. Since φ_i maps $\mathfrak{A}$ onto $\mathfrak{A}/M_i$, it follows that $\psi_i \circ \varphi$ must also map $\mathfrak{A}$ onto $\mathfrak{A}/M_i$. Consequently, φ is a subdirect representation of $\mathfrak{A}$. □

It is worth pointing out, if only to avoid later confusion, that the preceding theorem applies in particular to degenerate relation algebras. In fact, a degenerate relation algebra is isomorphic to the subdirect product of the empty system of simple relation algebras.

Theorem 12.10 has important implications for the validity of equations and, more generally, conditional equations in relation algebras.

Theorem 12.11. *An equation or conditional equation is true in all relation algebras if and only if it is true in all simple relation algebras.*

Proof. Formulas that are equations or conditional equations are preserved under the formation of direct products and subalgebras, by Lemmas 11.17(ii) and 11.18(ii) (together with the remark following

the latter lemma). If such a formula is true in all simple relation algebras, then it is true in all direct products of simple relation algebras, and therefore in all subalgebras of such products. Since every relation algebra is isomorphic to a subdirect product of simple relation algebras, by Theorem 12.10, it follows that the formula must be true in all relation algebras. On the other hand, if the formula is true in all relation algebras, then in particular it is true in all simple relation algebras. □

12.4 Historical remarks

The notion of a weak direct product—or a *direct sum*, as it is sometimes called—seems to have first arisen in group theory in the 1920s and 1930s. For groups (with or without operators), the internal form of the construction is often used. Weak direct products of Boolean algebras were mentioned briefly in Halmos [40] and, according to Ildikó Sain, were later studied by Monk around 1979. Sain [94] introduced a general notion of the weak direct product of a system of arbitrary algebras of the same similarity type. Weak direct products of relation algebras were first studied in Givant [34], which discusses both the external and the internal versions of the construction; Lemma 12.1, Theorem 12.2 and Corollary 12.3 are from that work. Ample internal products are also considered in [34], where versions of Lemma 12.6 and Theorem 12.7 may be found.

Subdirect products were first considered by Amalie Emmy Noether in the 1920s in the context of rings, and were later studied in that context by Gottfried Maria Hugo Köthe [59] and Neal Henry McCoy [81], among others. The general algebraic notions of a subdirect product, a subdirect representation, and a subdirectly irreducible algebra are due to Birkhoff. In [13] (see also [11]), he gives versions of Theorem 12.8 and the equivalence of (i) and (ii) in Lemma 12.9 that are applicable to arbitrary algebras (see Exercises 12.17 and 12.18), and he proves that an arbitrary algebra is always isomorphic to a subdirect product of subdirectly irreducible algebras (see Exercise 12.21). The characterizations of subdirectly irreducible relation algebras given in parts (iii) and (iv) of Lemma 12.9 are due to Givant. The Semi-simplicity Theorem 12.10 is due to Jónsson and Tarski [55], and the conclusion drawn in Theorem 12.11 was observed by Tarski in [112], if not earlier.

Exercises

12.1. Fill in the missing details in the proof of Lemma 12.1.

12.2. Suppose $\mathfrak{A}$ is the weak external product, and $\mathfrak{B}$ a weak internal product, of a system of relation algebras $(\mathfrak{A}_i : i \in I)$. Prove that the function mapping each element $r = (r_i : i \in I)$ in $\mathfrak{A}$ to the sum $\sum_i r_i$ is an isomorphism from $\mathfrak{A}$ to $\mathfrak{B}$. Conclude that two weak internal products of a system of relation algebras are always isomorphic via a mapping that is the identity function on the universe of each factor algebra. This justifies speaking of *the* internal weak product of the system.

12.3. Prove that the weak internal product of a system of relation algebras exists if and only if the algebras are disjoint except for a common zero.

12.4. Fill in the missing details in the proof of Theorem 12.2.

12.5. Formulate and prove an external version of Theorem 12.2.

12.6. Prove Lemma 12.4.

12.7. Prove Lemma 12.5.

12.8. Formulate and prove a version of Lemma 11.19 that applies to weak products.

12.9. Formulate and prove a version of Corollary 11.20 that applies to weak products.

12.10. Suppose $\mathfrak{A}$ is the direct product, and $\mathfrak{B}$ the weak direct product, of a system of relation algebras. Prove that any complete subalgebra of $\mathfrak{A}$ that includes $\mathfrak{B}$ as a subalgebra must coincide with $\mathfrak{A}$.

12.11. Formulate and prove a version of Lemma 11.48 that applies to weak internal products.

12.12. Suppose $\mathfrak{A}$ is the direct product of a system $(\mathfrak{A}_i : i \in I)$ of relation algebras. There is another subalgebra of $\mathfrak{A}$ that is a natural candidate for the weak direct product of the system. It's universe is the set B consisting of those elements $r = (r_i : i \in I)$ in $\mathfrak{A}$ such that r_i belongs to the minimal subalgebra of $\mathfrak{A}_i$ for all but finitely

many indices i. Prove that B really is a subuniverse of $\mathfrak{A}$. Write $\mathfrak{B}$ for the corresponding subalgebra of $\mathfrak{A}$, and write $\mathfrak{C}$ for the subalgebra of $\mathfrak{A}$ that is the weak direct product of the system $(\mathfrak{A}_i : i \in I)$, as defined after Lemma 12.1. Prove that $\mathfrak{C}$ is a subalgebra of $\mathfrak{B}$. Give an example for which all three algebras $\mathfrak{A}$, $\mathfrak{B}$, and $\mathfrak{C}$ are distinct.

12.13. Prove that every ample internal product of a system of relation algebras is isomorphic to a subalgebra of the external product of the system, and in fact to a subalgebra that includes the weak external product as a subalgebra.

12.14. Fill in the missing details in the proof of Lemma 12.6.

12.15. Prove Theorem 12.7.

12.16. Prove that a subdirectly irreducible relation algebra is simple by using the equivalence of (i) and (ii) in Lemma 12.9, the Lattice of Ideals Theorem 8.26, and the fact that a Boolean algebra is subdirectly irreducible if and only if it has exactly two elements.

12.17. Prove that an arbitrary algebra $\mathfrak{A}$ is isomorphic to a subdirect product of a system $(\mathfrak{A}_i : i \in I)$ of algebras (of the same similarity type as $\mathfrak{A}$) if and only if there is a system $(\Theta_i : i \in I)$ of congruences on $\mathfrak{A}$ such that $\bigcap_i \Theta_i = id_A$ and $\mathfrak{A}_i$ is isomorphic to the quotient $\mathfrak{A}_i/\Theta_i$ for each i.

12.18. Prove that an arbitrary algebra $\mathfrak{A}$ is subdirectly irreducible if and only if it has a smallest congruence that is different from id_A.

12.19. Prove for arbitrary algebras that a simple algebra is always subdirectly irreducible, and a subdirectly irreducible algebra is always directly indecomposable. Show that the reverse implications fail in general.

12.20. Prove that for each pair of elements (r, s) in an arbitrary algebra $\mathfrak{A}$, there is a maximal congruence Θ on $\mathfrak{A}$ that does not contain the pair (r, s).

12.21. Prove that an arbitrary algebra $\mathfrak{A}$ is isomorphic to a subdirect product of subdirectly irreducible algebras.

12.22. Prove, in the context of arbitrary algebras, that an equation is true in a subdirect product if and only if it is true in each of the subdirect factors of the product.

Chapter 13
Minimal relation algebras

A relation algebra is said to be *minimal* if it is generated by the empty set, or equivalently, if it is generated by the identity element. These algebras were already discussed in Section 6.7 in the context of minimal subalgebras; however, that discussion was necessarily incomplete because the tools required for a systematic analysis of these algebras were not yet available. What is needed for such an analysis is a form of the Product Decomposition Theorem—say, the internal form given in Theorem 11.39—and Theorem 12.11. The main goal of this chapter is a complete structural analysis of all minimal relation algebras.

13.1 Types

A relation algebra is said to be of *type one*, *two*, or *three* respectively according to whether the equation

$$0' ; 0' = 0, \qquad 0' ; 0' = 1', \qquad \text{or} \qquad 0' ; 0' = 1$$

holds in it. Type one relation algebras can be characterized by several other properties.

Lemma 13.1. *The following conditions on a relation algebra $\mathfrak{A}$ are equivalent.*

(i) $\mathfrak{A}$ *is of type one.*
(ii) $\mathfrak{A}$ *is a Boolean relation algebra.*
(iii) $1' = 1$.
(iv) $0' = 0$.

S. Givant, *Introduction to Relation Algebras*,
DOI 10.1007/978-3-319-65235-1_13

Proof. The equivalence of conditions (ii)–(iv) follows by Boolean algebra and Lemma 3.1, and condition (iv) implies condition (i), by Corollary 4.17. It therefore suffices to prove that condition (i) implies condition (iv). Assume $\mathfrak{A}$ is of type one, so that

$$0\text{'} \,;\, 0\text{'} = 0. \tag{1}$$

In this case,

$$1 \,;\, 0\text{'} = (1\text{'} + 0\text{'}) \,;\, 0\text{'} = 1\text{'} \,;\, 0\text{'} + 0\text{'} \,;\, 0\text{'} = 0\text{'} + 0\text{'} \,;\, 0\text{'} = 0\text{'} + 0\text{'} = 0\text{'}, \tag{2}$$

by Boolean algebra, the distributive and identity laws for relative multiplication, and (1). Assumption (1) and Boolean algebra imply that

$$(0\text{'} \,;\, 0\text{'}) \cdot 1 = 0.$$

Apply the De Morgan-Tarski laws (Lemma 4.8, with 0' in place of r and s, and 1 in place of t) and Lemma 4.7(vi) to arrive at

$$(1 \,;\, 0\text{'}) \cdot 0\text{'} = 0.$$

Combine this last equation with (2) to conclude that $0\text{'} = 0$. □

All three of the type equations hold in degenerate relation algebras, so such algebras may be assigned all three types. A non-degenerate relation algebra, however, has at most one type. To see this, observe that a relation algebra is degenerate if and only if $0 = 1\text{'}$. Indeed, if this equation holds, then

$$0 = 1 \,;\, 0 = 1 \,;\, 1\text{'} = 1,$$

by Corollary 4.17, the given assumption, and the identity law for relative multiplication; consequently, the relation algebra is degenerate. The reverse implication is trivial. It follows that if $1\text{'} \neq 1$ in a non-degenerate relation algebra, then the three elements 0, 1', and 1 are distinct from one another, so the validity of any one of the type equations precludes the validity of the other two. On the other hand, if $1\text{'} = 1$ in a non-degenerate relation algebra, then $0 = 0\text{'}$, by Boolean algebra, and therefore the second and third type equations cannot be valid, by Corollary 4.17.

It may happen of course that none of the above equations holds in a given relation algebra, in which case no type is assigned to the algebra. But simple relation algebras do have uniquely determined types.

Lemma 13.2. *Every simple relation algebra has a unique type.*

Proof. Let $\mathfrak{A}$ be a simple relation algebra. The proof that $\mathfrak{A}$ has a type splits into cases. If $0' = 0$, then $\mathfrak{A}$ is of type one, by Lemma 13.1.

Suppose next that $0' \neq 0$, but $(0';0')\cdot 0' = 0$. The assumed simplicity of $\mathfrak{A}$ implies that $1 ; 0' ; 1 = 1$, by the Simplicity Theorem 9.2, and therefore

$$\begin{aligned} 1 = 1 ; 0' ; 1 = (0' + 1') ; 0' ; 1 &= (0' ; 0' ; 1) + (1' ; 0' ; 1) \\ &= (0' ; 0' ; 1) + (0' ; 1), \end{aligned} \tag{1}$$

by Boolean algebra, and the distributive and identity laws for relative multiplication. Use the monotony law for relative multiplication and Lemma 4.5(iv) to get

$$0' ; 0' ; 1 \leq 0' ; 1 ; 1 = 0' ; 1. \tag{2}$$

Combine (1) and (2) to arrive at $1 = 0' ; 1$. This last equation, Boolean algebra, and the distributive and identity laws for relative multiplication, yield

$$1 = 0' ; 1 = 0' ; (0' + 1') = 0' ; 0' + 0' ; 1' = 0' ; 0' + 0'. \tag{3}$$

The elements $0' ; 0'$ and $0'$ are disjoint, by assumption, and they sum to one, by the preceding computation, so they form a partition of one. Consequently,

$$0' ; 0' = -0' = 1',$$

by Boolean algebra. Thus, $\mathfrak{A}$ is of type two.

Suppose finally that $(0' ; 0') \cdot 0' \neq 0$. The assumed simplicity of $\mathfrak{A}$ implies that

$$1 ; [(0' ; 0') \cdot 0'] ; 1 = 1, \tag{4}$$

by Theorem 9.2. Replace both occurrences of 1 on the left side of (4) with $0' + 1'$, and use the distributive law, to write $1 ; [(0' ; 0') \cdot 0'] ; 1$ as the sum of the four terms

$$\begin{array}{ll} 0' ; [(0' ; 0') \cdot 0'] ; 0', & \quad 1' ; [(0' ; 0') \cdot 0'] ; 0', \\ 0' ; [(0' ; 0') \cdot 0'] ; 1', & \quad 1' ; (0' ; 0') \cdot 0' ; 1'. \end{array}$$

These four terms simplify to

$$\begin{array}{ll} 0\text{'} \mathbin{;} [(0\text{'} \mathbin{;} 0\text{'}) \cdot 0\text{'}] \mathbin{;} 0\text{'}, & [(0\text{'} \mathbin{;} 0\text{'}) \cdot 0\text{'}] \mathbin{;} 0\text{'}, \\ 0\text{'} \mathbin{;} [(0\text{'} \mathbin{;} 0\text{'}) \cdot 0\text{'}], & (0\text{'} \mathbin{;} 0\text{'}) \cdot 0\text{'}, \end{array}$$

by the identity law for relative multiplication. Consequently, the last four terms sum to 1, by (4).

Obviously,

$$(0\text{'} \mathbin{;} 0\text{'}) \cdot 0\text{'} \le 0\text{'} \mathbin{;} 0\text{'} \qquad \text{and} \qquad (0\text{'} \mathbin{;} 0\text{'}) \cdot 0\text{'} \le 0\text{'}, \tag{5}$$

by Boolean algebra, Also,

$$0\text{'} \mathbin{;} 0\text{'} \mathbin{;} 0\text{'} \mathbin{;} 0\text{'} = 0\text{'} \mathbin{;} 0\text{'}, \tag{6}$$

by Lemma 4.34. Use (5), (6), and the monotony law for relative multiplication to arrive at

$$\begin{aligned} 0\text{'} \mathbin{;} [(0\text{'} \mathbin{;} 0\text{'}) \cdot 0\text{'}] \mathbin{;} 0\text{'} &\le 0\text{'} \mathbin{;} 0\text{'} \mathbin{;} 0\text{'} \mathbin{;} 0\text{'} = 0\text{'} \mathbin{;} 0\text{'}, \\ [(0\text{'} \mathbin{;} 0\text{'}) \cdot 0\text{'}] \mathbin{;} 0\text{'} &\le 0\text{'} \mathbin{;} 0\text{'}, \\ 0\text{'} \mathbin{;} [(0\text{'} \mathbin{;} 0\text{'}) \cdot 0\text{'}] &\le 0\text{'} \mathbin{;} 0\text{'}. \end{aligned}$$

Combine these observations with those of the previous paragraph to conclude that

$$1 \le 0\text{'} \mathbin{;} 0\text{'} + 0\text{'} \mathbin{;} 0\text{'} + 0\text{'} \mathbin{;} 0\text{'} + 0\text{'} \mathbin{;} 0\text{'} = 0\text{'} \mathbin{;} 0\text{'}.$$

Thus, $1 = 0\text{'} \mathbin{;} 0\text{'}$, so $\mathfrak{A}$ is of type three. □

When the algebra $\mathfrak{A}$ in the preceding proof is a full set relation algebra of the form $\mathfrak{Re}(U)$, the three cases of the proof correspond respectively to the cases when U has one element, two elements, and at least three elements. It follows that an example of a minimal, non-degenerate relation algebra of type n, for $n = 1, 2, 3$, is provided by the minimal set relation algebra $\mathfrak{M}_n$ constructed in Section 3.1. The next lemma says that, up to isomorphism, this is the only possible example.

Lemma 13.3. *A minimal, non-degenerate relation algebra of type n is isomorphic to $\mathfrak{M}_n$.*

Proof. Let $\mathfrak{A}$ be a minimal, non-degenerate relation algebra of type n. The proof that $\mathfrak{A}$ is isomorphic to $\mathfrak{M}_n$ splits into cases. If $n = 1$, then $\mathfrak{A}$ is a Boolean relation algebra, by Lemma 13.1. The set

$$B = \{0, 1\}$$

is a Boolean subuniverse, and therefore a relation algebraic subuniverse, of $\mathfrak{A}$, by the definition of a Boolean relation algebra. Since $\mathfrak{A}$ is assumed to be minimal, the subuniverse B must in fact coincide with the universe of $\mathfrak{A}$. The function that maps the zero and unit of $\mathfrak{A}$ to the zero and unit of $\mathfrak{M}_1$ is easily seen to be an isomorphism.

Assume next that $n = 2$, so that

$$0\text{'} \neq 0 \qquad \text{and} \qquad 0\text{'} \mathbin{;} 0\text{'} = 1\text{'}.$$

In this case, the constants 0, 1', 0', and 1 in $\mathfrak{A}$ are distinct (see the remarks preceding Lemma 13.2), and

$$0\text{'} \mathbin{;} 1 = 0\text{'} \mathbin{;} (0\text{'} + 1\text{'}) = 0\text{'} \mathbin{;} 0\text{'} + 0\text{'} \mathbin{;} 1\text{'} = 1\text{'} + 0\text{'} = 1,$$

by Boolean algebra, the distributive and identity laws for relative multiplication, and the assumption that $\mathfrak{A}$ is of type two. The relative product of any two of the four constants is therefore determined by the relative multiplication table in Table 13.1. The sum of any two

+	0	1'	0'	1
0	0	1'	0'	1
1'	1'	1'	1	1
0'	0'	1	0'	1
1	1	1	1	1

;	0	1'	0'	1
0	0	0	0	0
1'	0	1'	0'	1
0'	0	0'	1'	1
1	0	1	1	1

Table 13.1 Addition and relative multiplication tables for the constants in an algebra of type 2.

of the four constants is obviously determined by the addition table in Table 13.1.

The entries in these two tables are all elements of the set

$$B = \{0, 1\text{'}, 0\text{'}, 1\}, \tag{1}$$

so this set is closed under addition and relative multiplication. Clearly, this set is also closed under complement, and it is closed under converse because each element in B is its own converse (see Lemmas 4.1(vi), 4.3, and 4.7(vi)). It follows that B is a subuniverse of $\mathfrak{A}$. Since $\mathfrak{A}$ is assumed to be minimal, the subuniverse B must in fact coincide with the universe of $\mathfrak{A}$. A comparison of the addition and relative multiplication tables for $\mathfrak{A}$ and for $\mathfrak{M}_2$ shows that the function mapping the constants

in $\mathfrak{A}$ to the corresponding constants in $\mathfrak{M}_2$ preserves the operations of addition and relative multiplication, and is therefore an isomorphism, by the remarks preceding Lemma 7.7.

The argument for the case when $n = 3$ is similar to the preceding argument. In this case, the constants 0, 1', 0', and 1 are again distinct, and

$$1 = 0' \,;\, 0' \leq 0' \,;\, 1,$$

so that 0';1 = 1. The relative product of any two of the four constants is therefore determined by the relative multiplication table in Table 13.2. Addition is determined by the addition table in Table 13.1. Just as in

;	0	1'	0'	1
0	0	0	0	0
1'	0	1'	0'	1
0'	0	0'	1	1
1	0	1	1	1

Table 13.2 Relative multiplication table for the constants in an algebra of type 3.

the previous case, these tables and some straightforward considerations imply that the set of constants in (1) is closed under the operations of $\mathfrak{A}$ and is therefore the universe of $\mathfrak{A}$, by the assumed minimality of $\mathfrak{A}$. The algebra $\mathfrak{M}_3$ has the same number of elements as $\mathfrak{A}$ and the same addition and relative multiplication tables as $\mathfrak{A}$, so the function mapping the constants in $\mathfrak{A}$ to the corresponding constants in $\mathfrak{M}_3$ is an isomorphism. □

The preceding two lemmas already yield a description of the simple minimal relation algebras.

Theorem 13.4. *The simple minimal relation algebras are*, *up to isomorphism*, *precisely the algebras* $\mathfrak{M}_1$, $\mathfrak{M}_2$, *and* $\mathfrak{M}_3$.

Proof. A simple minimal relation algebra must be of type one, two, or three, by Lemma 13.2, and therefore must be isomorphic to one of the three given minimal set relation algebras, by Lemma 13.3. □

13.2 Type decomposition

Lemma 13.2 says that every simple relation algebra is of one of the three types. The next theorem—the *Type Decomposition Theorem*—says that every relation algebra (and not just every minimal relation algebra) can be written as a product of algebras of the three types.

Theorem 13.5. *Every relation algebra* $\mathfrak{A}$ *can be written as the internal product of three relation algebras*,

$$\mathfrak{A} = \mathfrak{A}_1 \otimes \mathfrak{A}_2 \otimes \mathfrak{A}_3,$$

of types one, *two*, *and three respectively*.

Proof. Define elements u_1, u_2, and u_3 in an arbitrary relation algebra by

$$u_3 = 1 ; [(0\text{'} ; 0\text{'}) \cdot 0\text{'}] ; 1, \tag{1}$$
$$u_2 = (1 ; 0\text{'} ; 1) \cdot -u_3, \tag{2}$$
$$u_1 = -u_2 \cdot -u_3. \tag{3}$$

We shall show that the equations

$$(0\text{'} \cdot u_1) ; (0\text{'} \cdot u_1) = 0, \tag{4}$$
$$(0\text{'} \cdot u_2) ; (0\text{'} \cdot u_2) = 1\text{'} \cdot u_2, \tag{5}$$
$$(0\text{'} \cdot u_3) ; (0\text{'} \cdot u_3) = u_3 \tag{6}$$

hold in the algebra.

Assume first that the algebra is simple. Under this assumption, the algebra must be of type one, two, or three, by Lemma 13.2. If it is of type two, then

$$0\text{'} \neq 0 \qquad \text{and} \qquad (0\text{'} ; 0\text{'}) \cdot 0\text{'} = 0, \tag{7}$$

and therefore

$$u_3 = 1 ; [(0\text{'} ; 0\text{'}) \cdot 0\text{'}] ; 1 = 1 ; 0 ; 1 = 0, \tag{8}$$
$$u_2 = (1 ; 0\text{'} ; 1) \cdot -u_3 = 1 \cdot 1 = 1, \tag{9}$$
$$u_1 = -u_2 \cdot -u_3 = 0 \cdot 1 = 0, \tag{10}$$

by (1)–(3), (7), the assumption of simplicity, and the Simplicity Theorem 9.2. The validity of equations (4)–(6) in this case is now immediate:

in view of (10) and (8), equations (4) and (6) both reduce to the equation $0;0 = 0$, which holds by Corollary 4.17; in view of (9), equation (5) reduces to the equation $0';0' = 1'$, which holds by the assumption that the algebra is of type two. The cases when the algebra is of type one or type three are treated in a completely analogous fashion, and are left as an exercise. The preceding arguments show that equations (4)–(6) hold in all simple relation algebras. Consequently, these equations hold in all relation algebras, by Theorem 12.11.

Fix an arbitrary relation algebra $\mathfrak{A}$, and let (1)–(3) be elements defined in $\mathfrak{A}$. These elements are clearly disjoint and sum to 1, by Boolean algebra, so they form a partition of the unit in $\mathfrak{A}$. The first of them is an ideal element, by Lemma 5.38(ii), so the other two must be ideal elements, by Lemma 5.39(iii),(iv). Consequently, they form an orthogonal system of ideal elements, by Corollary 11.29. Write

$$\mathfrak{A}_n = \mathfrak{A}(u_n)$$

for $n = 1, 2, 3$, and apply the Internal Product Decomposition Theorem 11.39 to conclude that

$$\mathfrak{A} = \mathfrak{A}_1 \otimes \mathfrak{A}_2 \otimes \mathfrak{A}_3.$$

The diversity and zero elements in $\mathfrak{A}_1$ are $0' \cdot u_1$ and 0 respectively, so equation (4) implies that $\mathfrak{A}_1$ is of type one. The diversity and identity elements in $\mathfrak{A}_2$ are $0' \cdot u_2$ and $1' \cdot u_2$ respectively, so equation (5) implies that $\mathfrak{A}_2$ is of type two. The diversity and unit elements in $\mathfrak{A}_3$ are $0' \cdot u_3$ and u_3 respectively, so equation (6) implies that $\mathfrak{A}_3$ is of type three.

□

To illustrate the preceding theorem and its proof, consider an arbitrary equivalence relation E on a set U. Let K_1, K_2, and K_3 be the sets of equivalence classes of E with exactly one element, exactly two elements, and at least three elements respectively. In the full set relation algebra $\mathfrak{A} = \mathfrak{Re}(E)$, the ideal element u_n defined in the preceding proof is just the relation

$$E_n = \bigcup\{V \times V : V \in K_n\}.$$

The proof of the theorem shows that the relativization

$$\mathfrak{A}_n = \mathfrak{A}(E_n) = \mathfrak{Re}(E_n)$$

has type n, and that $\mathfrak{A}$ is the internal product of the three relativizations $\mathfrak{A}_1$, $\mathfrak{A}_2$, and $\mathfrak{A}_3$. Consequently, the decomposition given by the theorem is

$$\mathfrak{Re}(E) = \mathfrak{Re}(E_1) \otimes \mathfrak{Re}(E_2) \otimes \mathfrak{Re}(E_3).$$

It may be of some interest to the reader to compare this decomposition with the one given by the Relativization Decomposition Theorem 11.40.

13.3 Classification of minimal relation algebras

We are now in a position to describe all minimal relation algebras.

Theorem 13.6. *The minimal relation algebras are, up to isomorphism, precisely the eight different possible products of the minimal set relation algebras $\mathfrak{M}_1$, $\mathfrak{M}_2$, and $\mathfrak{M}_3$, with each factor occurring at most once.*

Proof. It is not difficult to verify that each of the seven products

$$\begin{gathered}\mathfrak{M}_1, \qquad \mathfrak{M}_2, \qquad \mathfrak{M}_3,\\ \mathfrak{M}_1 \times \mathfrak{M}_2, \qquad \mathfrak{M}_1 \times \mathfrak{M}_3, \qquad \mathfrak{M}_2 \times \mathfrak{M}_3,\\ \mathfrak{M}_1 \times \mathfrak{M}_2 \times \mathfrak{M}_3,\end{gathered}$$

as well as the product $\mathfrak{M}_0$ of the empty system of relation algebras, is a minimal relation algebra. Consider, as a concrete example, the product

$$\mathfrak{A} = \mathfrak{M}_1 \times \mathfrak{M}_2 \times \mathfrak{M}_3.$$

The ideal elements u_1, u_2, and u_3 in $\mathfrak{A}$ from (1)–(3) in the proof of the preceding theorem are the units of the internal factors corresponding to $\mathfrak{M}_1$, $\mathfrak{M}_2$, and $\mathfrak{M}_3$, and these ideal elements are clearly generated by the identity element 1' of $\mathfrak{A}$. For $n = 1, 2, 3$, the identity element of the internal factor corresponding to $\mathfrak{M}_n$ is $1' \cdot u_n$, and this relativized identity element is generated by 1' as well, by the definition of u_n. Since $1' \cdot u_n$ generates all of the elements in the internal factor corresponding to $\mathfrak{M}_n$, it follows that 1' generates all of the elements in $\mathfrak{A}$. Consequently, $\mathfrak{A}$ is minimal.

Suppose now that $\mathfrak{A}$ is an arbitrary minimal relation algebra. Apply the Type Decomposition Theorem 13.5 to write $\mathfrak{A}$ as an internal product

$$\mathfrak{A} = \mathfrak{A}_1 \otimes \mathfrak{A}_2 \otimes \mathfrak{A}_3, \tag{1}$$

where $\mathfrak{A}_n$ is of type n for $n = 1, 2, 3$. Each of the factors $\mathfrak{A}_n$ must itself be a minimal relation algebra. Indeed, if one of them, say $\mathfrak{A}_2$, were not minimal, then it would have a proper subalgebra $\mathfrak{B}_2$, and the product $\mathfrak{A}_1 \otimes \mathfrak{B}_2 \otimes \mathfrak{A}_3$ would be a proper subalgebra of $\mathfrak{A}$, by the internal version of Corollary 11.20, contradicting the assumption that $\mathfrak{A}$ is minimal. Since $\mathfrak{A}_n$ is minimal and of type n, it is either degenerate, in which case it can be omitted from the decomposition, or else it is isomorphic to $\mathfrak{M}_n$, by Lemma 13.3. Conclusion: omitting the degenerate factors in (1), we obtain a representation of $\mathfrak{A}$ as a product in which each factor is isomorphic to one of minimal relation algebras $\mathfrak{M}_1$, $\mathfrak{M}_2$, and $\mathfrak{M}_3$, and no two factors are isomorphic to the same minimal algebra. If all of the factors in (1) are degenerate, and therefore omitted, then $\mathfrak{A}$ must be the product of the empty system of relation algebras; in this case, $\mathfrak{A}$ is degenerate and therefore isomorphic to $\mathfrak{M}_0$. □

Each of the minimal relation algebras described in the preceding theorem has a set-theoretic realization as an algebra of relations. This already follows from the set-theoretical definition of the algebras $\mathfrak{M}_n$ at the end of Section 3.1 and from the discussion preceding Definition 11.34. Here is a more direct argument. The minimal algebras $\mathfrak{M}_n$ with $n = 0, 1, 2, 3$ are, by definition, set relation algebras. For the products

$$\mathfrak{A} = \mathfrak{M}_m \times \mathfrak{M}_n$$

with $1 \leq m < n \leq 3$, take E_{mn} to be an equivalence relation on a set with $m+n$ elements such that E_{mn} has exactly two equivalence classes, one with m elements and the other with n elements. The subalgebra of $\mathfrak{Re}(E_{mn})$ generated by the empty set is isomorphic to $\mathfrak{A}$. For the product

$$\mathfrak{A} = \mathfrak{M}_1 \times \mathfrak{M}_2 \times \mathfrak{M}_3,$$

take E to be an equivalence relation on a set with six elements such that E has exactly three equivalence classes, one with one element, one with two elements, and one with three elements. The subalgebra of $\mathfrak{Re}(E)$ generated by the empty set is isomorphic to $\mathfrak{A}$.

Certain relative products $r_i \mathbin{;} r_j$ played an important role in the proof of Theorem 6.23. A few of these products are rather cumbersome to compute directly from the laws given in Chapter 4, but with the

hindsight of Theorem 13.6 they are easy to compute. Consider, for example, the product

$$r_1 \mathbin{;} r_3 = [(0\text{'} \mathbin{;} 0\text{'}) \cdot 0\text{'}] \mathbin{;} [-(0\text{'} \mathbin{;} 0\text{'}) \cdot 0\text{'}].$$

In $\mathfrak{M}_1$, this relative product reduces to $0 \mathbin{;} 0$, which is 0; in $\mathfrak{M}_2$, it reduces to $0 \mathbin{;} 0\text{'}$, which is 0; and in $\mathfrak{M}_3$, it reduces to $0\text{'} \mathbin{;} 0$, which is 0. The equation $r_1 \mathbin{;} r_3 = 0$ therefore holds in $\mathfrak{M}_n$ for each $n = 1, 2, 3$, so it holds in every direct product of these algebras. Apply Theorem 13.6 and Lemma 11.2(ii) to conclude that this equation holds in all minimal relation algebras, and therefore in all relation algebras (since it involves only individual constant symbols, and has no variables).

To give one more example, consider the relative product

$$r_2 \mathbin{;} r_2 = [(r_1 \mathbin{;} 1) \cdot 1\text{'}] \mathbin{;} (r_1 \mathbin{;} 1) \cdot 1\text{'}],$$

where $r_1 = (0\text{'} \mathbin{;} 0\text{'}) \cdot 0\text{'}$. In $\mathfrak{M}_1$ and $\mathfrak{M}_2$, the element r_1, and therefore also its domain r_2, is 0. In $\mathfrak{M}_3$, the element r_1 is 0', so its domain r_2 is 1'. It follows that $r_2 \mathbin{;} r_2$ is 0 in $\mathfrak{M}_1$ and $\mathfrak{M}_2$, and 1' in $\mathfrak{M}_3$. In other words, this relative product has the same value as r_2 in each of these algebras, so the equation $r_2 \mathbin{;} r_2 = r_2$ holds in $\mathfrak{M}_n$ for each $n = 1, 2, 3$. Apply Theorem 13.6 and Lemma 11.2(ii) to conclude that this equation holds in every minimal relation algebra, and therefore in every relation algebra.

13.4 Classification of algebras of types one and two

It is not difficult to construct a plethora of relation algebras of types one, two, and three. For example, every subdirect product of simple relation algebras of type n is a relation algebra of type n, because equations—and in particular, the equations specifying the type of a relation algebra—are preserved under the formation of direct products and subalgebras.

This observation raises the natural problem of describing the simple relation algebras of type n. For type three, the problem seems hopelessly difficult: every subalgebra of a full set relation algebra on a set of cardinality at least three is an example of a simple relation algebra of type three, and an explicit description of all of these algebras appears to be impossible. Somewhat surprisingly, a concrete description of the

simple relation algebras of types one and two is not only possible, but relatively easy.

We begin with two lemmas concerning identity singletons. An *identity singleton*, or a *point*, is a non-zero element x with the property that

$$x\,;1\,;x \leq 1\text{'}.$$

In a proper relation algebra on a set U, a relation R is a identity singleton just in case $R = \{(\alpha, \alpha)\}$ for some element α in U.

Lemma 13.7. *If x is an identity singleton in a simple relation algebra $\mathfrak{A}$, then $x\,;1\,;x = x \leq 1\text{'}$, and the relativization $\mathfrak{A}(x\,;1\,;x)$ is isomorphic to $\mathfrak{M}_1$.*

Proof. Assume x is an identity singleton. Observe first of all that

$$\begin{aligned} x \leq (x\,;1)\cdot(1\,;x) = x\,;1\,;x = (x\,;1\,;x)\cdot 1\text{'} \\ = x\,;1\text{'}\,;x = x\cdot 1\text{'}\cdot x = x, \end{aligned}$$

by Lemma 4.5(iii) and its first dual, Lemma 4.26, the assumption that x is an identity singleton and therefore the square $x\,;1\,;x$ is below 1', Lemma 5.54, Lemma 5.20(i), and Boolean algebra. Consequently,

$$x = x\,;1\,;x = (x\,;1\,;x)\cdot 1\text{'}. \tag{1}$$

A square is always an equivalence element, by Lemma 5.64, so it makes sense to speak of the relativization $\mathfrak{A}(x\,;1\,;x)$. The algebra $\mathfrak{A}$ is assumed to be simple, and the relativization of a simple relation algebra to a non-zero square is always simple, by Lemma 10.8, so the relativization $\mathfrak{A}(x\,;1\,;x)$ is simple. The identity element and unit of this relativization are, by definition, the elements

$$(x\,;1\,;x)\cdot 1\text{'} \qquad \text{and} \qquad x\,;1\,;x.$$

Since these two elements are equal, by (1), the algebra $\mathfrak{A}(x\,;1\,;x)$ is also a Boolean relation algebra, by Lemma 3.1(iii). A Boolean relation algebra is simple if and only if it is isomorphic to $\mathfrak{M}_1$, by the remarks preceding Corollary 9.4. Combine these observations to conclude that $\mathfrak{A}(x\,;1\,;x)$ is isomorphic to $\mathfrak{M}_1$. □

The lemma implies that an identity singleton x is an atom in the relativization $\mathfrak{A}(x;1;x)$, and therefore also an atom in $\mathfrak{A}$, by Lemma 10.5.

Corollary 13.8. *An identity singleton in a simple relation algebra is always an atom.*

The next lemma may be viewed as a generalization of this corollary to rectangles with atomic sides when at least one of the sides is an identity singleton.

Lemma 13.9. *If x is an identity singleton, and r an atom, in a simple relation algebra $\mathfrak{A}$, then the rectangles $x\,;1\,;r$ and $r\,;1\,;x$ are atoms in $\mathfrak{A}$, and they are equal if and only if $x = (r\,;1)\cdot 1' = (1\,;r)\cdot 1'$.*

Proof. The rectangle $x\,;1\,;r$ is certainly non-zero, by the Simplicity Theorem 9.2(iv) and the assumption that $\mathfrak{A}$ is simple. To prove that the rectangle is in fact an atom, consider any non-zero element $s \le x\,;1\,;r$, with the goal of showing that

$$s = x\,;1\,;r. \tag{1}$$

Since $(x\,;1\,;r)\cdot s \neq 0$, by assumption, we have $(1\,;x\,;s)\cdot r \neq 0$ by the De Morgan-Tarski laws (Lemma 4.8, with the elements $x\,;1$, r, and s in place of r, s, and t respectively) and Lemma 5.32(iii). Consequently,

$$r \le 1\,;x\,;s, \tag{2}$$

by the assumption that r is an atom. Form the relative product of both sides of (2) with $x\,;1$ on the left to arrive at

$$x\,;1\,;r \le x\,;1\,;(1\,;x\,;s) = x\,;1\,;x\,;s = x\,;s \le 1'\,;s = s,$$

by the monotony law for relative multiplication, Lemma 4.5(iv), the assumption that x is an identity singleton, and Lemma 13.7. Thus, (1) holds, so $x\,;1\,;r$ must be an atom.

The converse of an atom is an atom, by Lemma 4.1(vii), so $r^{\smile}$ is also an atom. Apply the observations of the preceding paragraph to $r^{\smile}$ instead of r to conclude that the rectangle $x;1;r^{\smile}$ is also an atom. The converse of this rectangle must again be an atom, by Lemma 4.1(vii). Since this converse is equal to $r\,;1\,;x$, by the involution laws, and Lemmas 4.1(vi) and 5.20(i) (with x in place of r), it follows that $r;1;x$ is an atom.

Write

$$y = (r\,;1)\cdot 1' \qquad \text{and} \qquad z = (1\,;r)\cdot 1', \tag{3}$$

and observe that

$$x\,;1\,;r = x\,;1\,;z \qquad \text{and} \qquad r\,;1\,;x = y\,;1\,;x, \tag{4}$$

by Corollary 5.27(iii) and its first dual. The rectangles

$$x\,;1\,;z \qquad \text{and} \qquad y\,;1\,;x$$

are equal if and only if $x = y$ and $z = x$, by Lemma 5.63(iii), so the rectangles

$$x\,;1\,;r \qquad \text{and} \qquad r\,;1\,;x$$

are equal if and only if

$$x = (r\,;1)\cdot 1' = (1\,;r)\cdot 1',$$

by (3) and (4). □

We come now to the description of the simple relation algebras of types one and two.

Theorem 13.10. *There is just one simple relation algebra of type one, up to isomorphism, namely $\mathfrak{M}_1$. There are just two simple relation algebras of type two, up to isomorphism, namely $\mathfrak{M}_2$ and the full set relation algebra on a two-element set.*

Proof. Consider first the case of type one. Certainly, $\mathfrak{M}_1$ is a simple relation algebra of type one, by Lemma 9.1 and the relative multiplication table for $\mathfrak{M}_1$. If $\mathfrak{A}$ is any simple relation algebra of type one, then

$$1' = 1 = 1'\,;1\,;1', \tag{1}$$

by Lemma 13.1 and the identity law for relative multiplication. It follows that 1' is an identity singleton, so the relativization of $\mathfrak{A}$ to the square $1';1;1'$ is isomorphic to $\mathfrak{M}_1$, by Lemma 13.7. This relativization coincides with $\mathfrak{A}$, by (1), so $\mathfrak{A}$ must be isomorphic to $\mathfrak{M}_1$.

Turn now to the type two case. The relation algebra $\mathfrak{M}_2$ is certainly simple and of type two, as is the full set relation algebra $\mathfrak{Re}(U)$ on a set U with two elements, say α and β. Consider an arbitrary simple relation algebra $\mathfrak{A}$ of type two. The defining equation for type two algebras and Lemma 4.7(vi) together imply that 0' is a function, since

$$0'^{\smile} ; 0' = 0' ; 0' = 1'.$$

Furthermore, 0' is non-zero by the assumption that $\mathfrak{A}$ is non-degenerate and of type two (see Lemma 13.1).

There are two possibilities. The first is that 1' is an atom. In this case, $\mathfrak{A}$ is an integral relation algebra, and therefore the non-zero function 0' is also an atom, by Integrality Theorem 9.7(vi). Thus, 1' and 0' form a partition of the unit in $\mathfrak{A}$ into atoms, so $\mathfrak{A}$ is an atomic relation algebra with two atoms, 1' and 0'. The relative multiplication table for these two atoms is given in Table 13.3.

;	1'	0'
1'	1'	0'
0'	0'	1'

Table 13.3 Relative multiplication table for atoms when $\mathfrak{A}$ is integral.

The atoms 1' and 0' in $\mathfrak{M}_2$ have the same relative multiplication table, so $\mathfrak{A}$ and $\mathfrak{M}_2$ must be isomorphic, by the version of the Atomic Isomorphism Theorem given in Corollary 7.12.

The other possibility is that 1' is not an atom. In this case, there must be non-zero subidentity elements x and y that partition 1'. Observe that

$$\begin{aligned} x ; 1 ; y = x ; (1' + 0') ; y &= (x ; 1' ; y) + (x ; 0' ; y) \\ &= (x \cdot 1' \cdot y) + (x ; 0' ; y) = 0 + (x ; 0' ; y) \\ &= x ; 0' ; y \leq 1' ; 0' ; 1' = 0', \end{aligned} \tag{2}$$

by Boolean algebra, the distributive law for relative multiplication, Lemma 5.20(i), the assumed disjointness of x and y, and the monotony and identity laws for relative multiplication. Exchange x and y in this argument to obtain

$$y ; 1 ; x \leq 0'. \tag{3}$$

The algebra $\mathfrak{A}$ is assumed to be simple, so

$$1 ; y ; 1 = 1, \tag{4}$$

by the Simplicity Theorem 9.2(ii). Consequently,

$$x\,;1\,;x = x\,;(1\,;y\,;1)\,;x = x\,;(1\,;y\,;y\,;1)\,;x$$
$$= (x\,;1\,;y)\,;(y\,;1\,;x) \le 0\text{'}\,;0\text{'} = 1\text{'},$$

by (4), Lemmas 5.11 and 5.8(ii), the associative law for relative multiplication, (2) and (3), the monotony law for relative multiplication, and the assumption that $\mathfrak{A}$ is of type two. This argument shows that x is an identity singleton, and therefore an atom, by Corollary 13.8. Exchange x and y in this argument to obtain that y is also an identity singleton and therefore an atom. Thus, x and y are atoms that partition the identity element in $\mathfrak{A}$.

The rectangles $x\,;1\,;y$ and $y\,;1\,;x$ are both atoms and they are distinct from one another, by Lemma 13.9 (with y in place of r). They are both below 0', by (2) and (3), so they must also be distinct from the identity singleton atoms

$$x\,;1\,;x = x \qquad \text{and} \qquad y\,;1\,;y = y.$$

These four atoms partition the unit, because

$$1 = 1\text{'}\,;1\,;1\text{'} = (x+y)\,;1\,;(x+y)$$
$$= (x\,;1\,;x) + (x\,;1\,;y) + (y\,;1\,;x) + (y\,;1\,;y)$$
$$= x + (x\,;1\,;y) + (y\,;1\,;x) + y.$$

Consequently, $\mathfrak{A}$ is atomic with exactly four atoms. The relative multiplication table for these atoms is given in Table 13.4; the various entries follow readily from Lemma 5.20(i) (or Corollary 5.60) and Corollary 5.62.

$;$	x	y	$x\,;1\,;y$	$y\,;1\,;x$
x	x	0	$x\,;1\,;y$	0
y	0	y	0	$y\,;1\,;x$
$x\,;1\,;y$	0	$x\,;1\,;y$	0	x
$y\,;1\,;x$	$y\,;1\,;x$	0	y	0

Table 13.4 Relative multiplication table for atoms when $\mathfrak{A}$ is not integral.

The atoms in the full set relation algebra $\mathfrak{Re}(U)$ are the singleton relations

$$\{(\alpha,\alpha)\}, \qquad \{(\beta,\beta)\}, \qquad \{(\alpha,\beta)\}, \qquad \{(\beta,\alpha)\},$$

and the relational composition table for these atoms is given in Table 13.5; the validity of the entries in this table follows immediately from the definition of relational composition.

$;$	$\{(\alpha,\alpha)\}$	$\{(\beta,\beta)\}$	$\{(\alpha,\beta)\}$	$\{(\beta,\alpha)\}$
$\{(\alpha,\alpha)\}$	$\{(\alpha,\alpha)\}$	0	$\{(\alpha,\beta)\}$	0
$\{(\beta,\beta)\}$	0	$\{(\beta,\beta)\}$	0	$\{(\beta,\alpha)\}$
$\{(\alpha,\beta)\}$	0	$\{(\alpha,\beta)\}$	0	$\{(\alpha,\alpha)\}$
$\{(\beta,\alpha)\}$	$\{(\beta,\alpha)\}$	0	$\{(\beta,\beta)\}$	0

Table 13.5 Relative multiplication table for the atoms in $\mathfrak{Re}(U)$.

A comparison of the two tables shows that the correspondence

$$\begin{aligned} x &\mapsto \{(\alpha,\alpha)\}, & x\,;1\,;y &\mapsto \{(\alpha,\beta)\} \\ y &\mapsto \{(\beta,\beta)\}, & y\,;1\,;x &\mapsto \{(\beta,\alpha)\} \end{aligned}$$

satisfies the conditions of Corollary 7.12. Apply the corollary to conclude that $\mathfrak{A}$ and $\mathfrak{Re}(U)$ are isomorphic. □

It is now possible to describe, up to isomorphism, all relation algebras of types one and two. As has already been pointed out, every subdirect product of a system of relation algebras of type n (for $n = 1, 2, 3$) is again a relation algebra of type n, because equational properties are preserved under subalgebras and direct products. On the other hand, if $\mathfrak{A}$ is a relation algebra of type n, then $\mathfrak{A}$ is isomorphic to a subdirect product of a system of simple relation algebras, by the Semi-simplicity Theorem 12.10. Each simple algebra in this system is a homomorphic image of $\mathfrak{A}$, by the definition of a subdirect product, so each of these algebras is also of type n, because equational properties are preserved under homomorphic images. Conclusion: a relation algebra $\mathfrak{A}$ is of type n if and only if $\mathfrak{A}$ is isomorphic to a subdirect product of simple relation algebras of type n. The simple relation algebras of types one and two are completely described in Theorem 13.10, so we obtain the following description of the relation algebras of types one and two.

Corollary 13.11. *The relation algebras of type one are, up to isomorphism, precisely the subdirect products of systems of algebras that are copies of $\mathfrak{M}_1$. The relation algebras of type two are, up to isomorphism, precisely the subdirect products of systems of algebras that are copies of $\mathfrak{M}_2$ and the full set relation algebra on a two-element set.*

The first conclusion of the corollary says, in essence, that every Boolean relation algebra is a subdirect product of the two-element Boolean relation algebra (see Lemma 13.1). This is just a relation algebraic form of the corresponding theorem about Boolean algebras.

13.5 Historical remarks

The notion of the type of a relation algebra was introduced by Jónsson and Tarski in [55] under the name *class*, and most of the results in this chapter concerning types are from that paper. This includes Lemmas 13.1 and 13.2, the Type Decomposition Theorem 13.5, the example following that theorem, the descriptions of relation algebras of types one and two contained in Theorem 13.10 and Corollary 13.11, and the observations in Exercises 13.5–13.7. The proof of Theorem 13.10 given here is due to Givant. The first assertion in Lemma 13.7, Corollary 13.8, and the first assertion in Lemma 13.9 are due to Maddux [75].

The problem of classifying minimal relation algebras is not discussed in [55]. It does arises implicitly in Tarski [111], and versions of Lemma 13.3 and Theorem 13.4 are given there. The classification of all minimal relation algebras that occurs in Theorem 13.6 appears to be due to Tarski and is contained in [112]. The classification of complete equational theories of relation algebras given in Exercises 13.11–13.13 is due to Tarski [111].

The notion of the type of an equivalence element, defined in Exercise 13.14, is due to Jónsson [51]. In that paper, Jónsson describes all relation algebras generated by a single equivalence element. The type decomposition theorem for equivalence elements given in Exercise 13.17, and the results implicit in Exercises 13.18–13.20, form the essential part of that description.

Exercises

13.1. Prove that the full set relation algebra on a set U has type one, two, or three according to whether the set U has exactly one element, exactly two elements, or at least three elements respectively.

13.2. Fill in the missing details in the proof of Lemma 13.3.

13.3. Fill in the missing details in the proof of Theorem 13.5.

13.4. Use arguments similar to the ones given at the end of Section 13.3 to verify each of the entries for the relative product $r_i \,;\, r_j$ in Table 6.1.

13.5. Prove that the inequality $0\text{'};0\text{'} \le 1\text{'}$ holds in a relation algebra $\mathfrak{A}$ if and only if $\mathfrak{A}$ is the internal product of a relation algebra of type one and a relation algebra of type two.

13.6. Prove that the inequality $0\text{'} \le 0\text{'};0\text{'}$ holds in a relation algebra $\mathfrak{A}$ if and only if $\mathfrak{A}$ is the internal product of a relation algebra of type one and a relation algebra of type three.

13.7. Prove that the inequality $1\text{'} \le 0\text{'};0\text{'}$ holds in a relation algebra $\mathfrak{A}$ if and only if $\mathfrak{A}$ is the internal product of a relation algebra of type two and a relation algebra of type three.

13.8. If u_2 and u_3 are the ideal elements defined at the beginning of the proof of Theorem 13.5, prove that the equation

$$0\text{'} \,;\, 0\text{'} = 1\text{'} \cdot u_2 + u_3$$

holds in every relation algebra.

13.9. Prove that, up to isomorphism, the only finite relation algebras with exactly two atoms are $\mathfrak{M}_2$, $\mathfrak{M}_3$, and $\mathfrak{M}_1 \times \mathfrak{M}_1$.

13.10. Prove that, up to isomorphism, the only finite relation algebra with exactly one atom is $\mathfrak{M}_1$.

13.11. Call

$$0\text{'} \,;\, 0\text{'} = 0, \qquad 0\text{'} \,;\, 0\text{'} = 1\text{'}, \qquad \text{and} \qquad 0\text{'} \,;\, 0\text{'} = 1$$

the *type one equation*, the *type two equation*, and the *type three equation* respectively. Prove that a relation algebra $\mathfrak{A}$ is isomorphic to $\mathfrak{M}_n$ (for $n = 1, 2, 3$) if and only if the type n equation and the *special equation*

$$r \,;\, 1 \,;\, -r \,;\, 1 \,;\, (r \cdot 1\text{'} + -r \cdot 0\text{'}) \,;\, 1 \,;\, (r \cdot 0\text{'} + -r \cdot 1\text{'}) = 0$$

(see Exercise 9.2) both hold in $\mathfrak{A}$, and $\mathfrak{A}$ is simple. Conclude that a relation algebra $\mathfrak{A}$ is isomorphic to a subdirect power of $\mathfrak{M}_n$ if and only if the type n equation and the special equation hold in $\mathfrak{A}$.

13.12. An equational theory $\mathcal{T}$ of relation algebras is said to be *maximal*, or *complete*, if it is not the inconsistent theory—that is to say, if it does not consist of all equations (in the language of relation algebras)—and if the only equational theory of relation algebras that properly includes $\mathcal{T}$ is the inconsistent theory. For $n = 1, 2, 3$, let $\mathcal{T}_n$ be the equational theory of the minimal relation algebra $\mathfrak{M}_n$, that is to say, $\mathcal{T}_n$ is the set of all equations true in $\mathfrak{M}_n$. Prove that the theory $\mathcal{T}_n$ is complete for each n, and that these are the only complete equational theories of relation algebras.

13.13. For $n = 1, 2, 3$, let $\mathcal{T}_n$ be the equational theory of the minimal relation algebra $\mathfrak{M}_n$ (see Exercise 13.12). Prove that $\mathcal{T}_n$ is axiomatized by the axioms of relation algebra, the type n equation, and the special equation (see Exercise 13.11).

13.14. Type decomposition can be extended from the identity element to arbitrary equivalence elements as follows. An equivalence element r is said to be of *type one*, *two*, or *three* respectively, according to which of the equations

$$(r \cdot 0') \mathbin{;} (r \cdot 0') = 0, \quad (r \cdot 0') \mathbin{;} (r \cdot 0') = r \cdot 1', \quad (r \cdot 0') \mathbin{;} (r \cdot 0') = r$$

holds. Prove that a (necessarily reflexive) equivalence relation R on a non-empty set U has type one, two, or three respectively in the full set relation algebra $\mathfrak{Re}(U)$ according to whether each equivalence class of R has exactly one element, exactly two elements, or at least three elements.

13.15. What can you say about the type (see Exercise 13.14) of the equivalence element 0?

13.16. Prove that every equivalence relation on a non-empty set is the union of three mutually disjoint set-theoretic equivalence elements of types one, two, and three respectively (see Exercise 13.14).

13.17. Prove that every equivalence element in a relation algebra is the sum of three mutually disjoint equivalence elements of types one, two, and three respectively (see Exercise 13.14). More concretely, for an arbitrary equivalence element r, define

$$\begin{aligned}
r_3 &= [(r \cdot 0') \mathbin{;} (r \cdot 0')] \mathbin{;} ([(r \cdot 0') \mathbin{;} (r \cdot 0')] \cdot 0'),\\
r_2 &= [r \mathbin{;} (r \cdot 0')] \cdot -r_3,\\
r_1 &= r \cdot -[r \mathbin{;} (r \cdot 0')].
\end{aligned}$$

Prove that r_1, r_2, and r_3 are equivalence elements of types one, two, and three respectively, and that these three equivalence elements are mutually disjoint and sum to r.

13.18. Prove that there are exactly two simple relation algebras generated by an equivalence element r of type two and exactly two simple relation algebras generated by an equivalence element r of type three, under the additional assumption that $1' < r < 1$.

13.19. Describe all simple relation algebras generated by a reflexive equivalence element.

13.20. Describe all simple relation algebras generated by an arbitrary equivalence element.

13.21. Prove that a relation R in a full set relation algebra $\mathfrak{Re}(U)$ is an identity singleton if and only if $R = \{(\alpha, \alpha)\}$ for some element α in U.

13.22. A *singleton* in a relation algebra is defined to be a non-zero element r satisfying the inequalities

$$r^{\smile} ; 1 ; r \leq 1' \qquad \text{and} \qquad r ; 1 ; r^{\smile} \leq 1'.$$

Prove that a relation R in a full set relation algebra $\mathfrak{Re}(U)$ is a singleton if and only if $R = \{(\alpha, \beta)\}$ for some elements α and β in U.

13.23. If r is a singleton (see Exercise 13.22) in a simple relation algebra, prove that the domain and range of r, that is to say, the elements

$$(r ; 1) \cdot 1' \qquad \text{and} \qquad (1 ; r) \cdot 1',$$

are identity singletons, and

$$r = [(r ; 1) \cdot 1'] ; [(1 ; r) \cdot 1'].$$

13.24. If an element r in a simple relation algebra can be written in the form $r = x ; 1 ; y$ for some identity singletons x and y, prove that r is a singleton (see Exercise 13.22) and that x and y are respectively the domain and range of r.

13.25. Describe the relations in a full set relation algebra $\mathfrak{Re}(U)$ that satisfy the inequality $r^{\smile} ; 1 ; r \leq 1'$. Describe the relations that satisfy the inequality $r ; 1 ; r^{\smile} \leq 1'$.

References

1. Abian, A.: Boolean rings with isomorphisms preserving suprema and infima. *London Mathematical Society* **3** (19713), pp. 618–620.
2. Andréka, H. and Givant, S.: Functionally dense relation algebras. *Algebra Universalis* **68** (2013), pp. 151–191.
3. Andréka, H., Givant, S., Jipsen, P., and Németi, I.: On Tarski's axiomatic foundations of the calculus of relations. *Journal of Symbolic Logic*, to appear.
4. Andréka, H., Givant, S., Mikulás, S., Németi, I., and Simon, A.: Notions of density that imply representability in algebraic logic. *Annals of Pure and Applied Logic* **91** (1998), pp. 93–190.
5. Andréka, H., Givant, S., and Németi, I.: The lattice of varieties of representable relation algebras. *Journal of Symbolic Logic* **59** (1994), pp. 631–661.
6. Andréka, H. and Maddux, R. D.: Representations for small relation algebras. *Notre Dame Journal of Formal Logic* **35** (1994), pp. 550–562.
7. Arrow, K. J.: A difficulty in the concept of social welfare. *Journal of Political Economy* **58** (1950), pp. 328–246.
8. Arrow, K. J.: *Social choice and individual values.* Third edition. Yale University Press, New Haven CN, 2012, xvi + 124 pp.
9. van Benthem, J. A. F. K.: *Language in action. Categories, lambdas and dynamic logic.* Studies in Logic and the Foundations of Mathematics, vol. 130, North Holland Publishing Company, Amsterdam, 1991, x + 349 pp.
10. Bird, R. and de Moor, O.: *Algebra of programming.* International Series in Computer Science, Prentice Hall, Upper Saddle River, NJ, 1997, 295 pp.

S. Givant, *Introduction to Relation Algebras*,
DOI 10.1007/978-3-319-65235-1

11. Birkhoff, G.: *Lattice theory.* First edition. American Mathematical Society Colloquium Publications, vol. 25, American Mathematical Society, Providence, RI, 1940, 155 pp.

12. Birkhoff, G.: On the structure of abstract algebras. *Proceedings of the Cambridge Philosophical Society* **31** (1944), pp. 433–454.

13. Birkhoff, G.: Subdirect unions in universal algebra. *Bulletin of the American Mathematical Society* **50** (1944), pp. 764–768.

14. Birkhoff, G.: Sobre los grupos de automorfismos. *Revista de la Unión Matemática Argentina* **110** (1946), pp. 155–157.

15. Boole, G.: *The mathematical analysis of logic—Being an essay towards a calculus of deductive reasoning.* MacMillan, Barclay, and MacMillan, Cambridge, 1847, 82 pp.

16. Boole, G.: *An investigation of the laws of thought, on which are founded the mathematical theories of logic and probabilities.* MacMillan and Company, Cambridge, and Walton and Maberly, London, 1854, v + iv + 424 pp.

17. Boyd, J.: The algebra of group kinship. *Journal of Mathematical Psychology* **6** (1969), pp. 139–167.

18. Brams, S. J. and Fishburn, P. C.: Approval voting. In: K. Arrow, A. Sen, and K. Suzumura (eds.) *Handbook of social choice and welfare*, Elsevier Science, Amsterdam, 2002, pp. 173–236.

19. Brink, C., Kahl, W., and Schmidt, G. (eds): *Relational methods in computer science.* Advances in Computing, Springer-Verlag, Vienna, 1997, xv + 274 pp.

20. Burris, S. and Sankappnavar, H. P.: *A course in universal algebra.* Graduate Texts in Mathematics, Springer-Verlag, New York, 1981, xvi + 276 pp.

21. Chang, C. C., Jónsson, B., and Tarski, A.: Refinement properties for relational structures. *Fundamenta Mathematicae* **55** (1964), pp. 249–281.

22. Chin, L. H.: *Distributive and modular laws in relation algebras.* Doctoral dissertation, University of California at Berkeley, Berkeley CA, 1948, 62 pp.

23. Chin, L. H. and Tarski, A.: Distributive and modular laws in the arithmetic of relation algebras. *University of California Publications in Mathematics, New Series* **1** (1951), pp. 341–384.

24. Comer, S.: Multivalued loops and their connection with algebraic logic. Unpublished manuscript, 1979, 173 pp.

25. Comer, S.: Multi-valued algebras and their graphical representation. Unpublished manuscript, 1986, 103 pp.

26. De Morgan, A.: On the syllogism, no. IV, and on the logic of relations. *Transactions of the Cambridge Philosophical Society* **10** (1864), pp. 331–358.

27. Dirichlet, J. P. G. L.: *Vorlesungen über Zahlentheorie.* Third edition, edited and with supplements by R. Dedekind, F. Vieweg und Sohn Verlag, Braunschweig, 1876.

28. Düntsch, I.: Relation algebras and their application in temporal and spatial reasoning. *Artificial Intelligence Review* **23** (2005), pp. 315–357.

29. Düntsch, I., Schmidt, G., and Winter, M.: A necessary relation algebra for mereotopology. *Studia Logica* **69** (2001), pp. 381–409.

30. Frias, M. F.: *Fork algebras in algebra, logic and computer science.* Advances in Logic, vol. 2, World Scientific Publishing Company, River Edge, NJ, 2002, xi + 217 pp.

31. Frobenius, G. and Stickelberger, L.: Über Gruppen von vertauschbaren Elementen. *Journal für die reine und angewandte Mathematik* **86** (1879), pp. 217–262.

32. Galvin, F.: *Horn sentences.* Doctoral dissertation, University of Minnesota, Minneapolis and St. Paul MN, (1965), iii + 47 pp.

33. Galvin, F.: Horn sentences. *Annals of Mathematical Logic* **1** (1970), pp. 389–422.

34. Givant, S.: *The structure of relation algebras generated by relativizations.* Contemporary Mathematics, vol. 156, American Mathematical Society, Providence RI, 1994, xvi + 134 pp.

35. Givant, S.: The calculus of relaltions as a foundation for mathematics. *Journal of Automated Reasoning* **37** (2006), pp. 277–322.

36. Givant, S.: *Duality theories for Boolean algebras with operators.* Springer Monographs in Mathematics, Springer-Verlag, New York, 2014, xiv + 233 pp.

37. Givant, S. and Andréka, H.: *Simple relation algebras.* Springer-Verlag, to appear.

38. Givant, S. and Halmos, P.: *Introduction to Boolean algebras.* Undergraduate Texts in Mathematics, Springer-Verlag, New York, 2009, xiv + 574 pp.

39. Grätzer, G.: *Universal algebra.* Second edition. Springer-Verlag, New York, 2008, xix + 586 pp.

40. Halmos, P.: *Lectures on Boolean algebras.* D. Van Nostrand Company, Princeton, NJ, 1963, vi + 147 pp.

41. Henkin, L., Monk, J. D., and Tarski, A.: *Cylindric algebras.* Part I. Studies in Logic and the Foundations of Mathematics, vol. 64, North-Holland Publishing Company, Amsterdam, 1971, vi + 508 pp.

42. Henkin, L., Monk, J. D., Tarski, A., Andréka, H., and Németi, I.: *Cylindric set algebras.* Lecture Notes in Mathematics, vol. 883, Springer-Verlag, Berlin Heidelberg New York, 1981, viii + 323 pp.

43. Hirsch, R. and Hodkinson, I.: Complete representations in algebraic logic. *Journal of Symbolic Logic* **62** (1997), pp. 816–847.

44. Hirsch, R. and Hodkinson, I.: *Relation algebras by games.* Studies in Logic and the Foundations of Mathematics, vol. 147, Elsevier Science, North-Holland Publishing Company, Amsterdam, 2002, 712 pp.

45. Hirsch, R., Hodkinson, I., and Maddux, R.: Provability with finitely many variables. *Bulletin of Symbolic Logic* **8** (2002), pp. 348–379.

46. Jipsen, P.: *Computer-aided investigations of relation algebras.* Doctoral dissertation, Vanderbilt University, Nashville TN, 1992, iii + 82 pp.

47. Jipsen, P.: Discriminator varieties of Boolean algebras with residuated operators. In: C. Rauszer (ed.), *Algebraic methods in logic and in computer science*, Banach Center Publications, vol. 28 (1993), Institute of Mathematics, Polish Academy of Sciences, pp. 239–252.

48. Jipsen, P. and Lukács, E.: Minimal relation algebras. *Algebra Universalis* **32** (1994), pp. 189–203.

49. Jónsson, B.: Representation of modular lattices and of relation algebras. *Transactions of the American Mathematical Society* **92** (1959), pp. 449–464.

50. Jónsson, B.: Varieties of relation algebras. *Algebra Universalis* **15** (1982), pp. 273–298.

51. Jónsson, B.: Relation algebras and Schröder categories. *Discrete Mathematics* **70** (1988), pp. 27–45.

52. Jónsson, B. and Tarski, A.: *Direct decompositions of finite algebraic systems.* Notre Dame Mathematical Lectures **5**, North State Press, Notre Dame, IN, 1947, vi + 64 pp.

53. Jónsson, B. and Tarski, A.: Representation problems for relation algebras. *Bulletin of the American Mathematical Society* **54** (1948), pp. 80 and 1192, Abstract 89.

54. Jónsson, B. and Tarski, A.: Boolean algebras with operators. Part I. *American Journal of Mathematics* **73** (1951), pp. 891–939.

55. Jónsson, B. and Tarski, A.: Boolean algebras with operators. Part II. *American Journal of Mathematics* **74** (1952), pp. 127–162.

56. Kahl, W. and Schmidt, G.:*Exploring (finite) relation algebras using tools written in Haskell.* Report Number 2000-02, Institute for Software Technology, Department of Computing Science, Federal Armed Forces University Munich, Munich, 2000, 158 pp.

57. Kamel, H.: *Relational algebra.* Doctoral dissertation, University of Pennsylvania, Philadelphia PA, 1952, viii + 161 pp.

58. Kamel, H.: Relational algebra and uniform spaces. *Journal of the London Mathematical Society* **29** (1954), pp. 342–344.

59. Köthe, G.: Abstrakte Theorie nichkommutative Ringe mit einer Anwendung auf die Darstellungstheorie kontinuierlicher Gruppen. *Mathematische Annalen* **103** (1930), pp. 545–572.

60. Kramer, R. L.: Relativized relation algebras. In: H. Andréka, J. D. Monk, and I. Németi (eds.), *Algebraic logic*, Colloquia Mathematica Societatis János Bolyai, vol. 54, North-Holland Publishing Company, Amsterdam, 1991, pp. 293–349.

61. Lambek, J.: Relations old and new. In: Orlowska, E. and Szalas, A.: *Relational methods for computer science applications*, Studies in Fuzziness and Soft Computing, Physica Verlag Rudolf Liebing KG, Vienna, 2001, pp. 135–148.

62. Langford, C. H.: Theorems on deducibility. *Annals of Mathematics*, Second Series **28** (1927), pp. 459–471.

63. Lewis, C. I.: *A survey of symbolic logic.* University of California Press, Berkeley, 1918, vi + 408 pp.

64. Lovász, L.: Operations with structures. *Acta Mathematica Academiae Scientiarum Hungaricae* **18** (1967), pp. 321–328.

65. Löwenheim, L.: Über Möglichkeiten im Relativkalkül. *Mathematische Annalen* **76** (1915), pp. 447–470.

66. Löwenheim, L.: Einkleidung der Mathematik in den Schöderschen Relativkalkül. *Journal of Symbolic Logic* **5**, pp. 1–15.

67. Lyndon, R. C.: The representation of relational algebras. *Annals of Mathematics*, series 2, **51** (1950), pp. 707–729.

68. Lyndon, R. C.: The representation of relational algebras, II. *Annals of Mathematics*, series 2, **63** (1956), pp. 294–307.

69. Lyndon, R. C.: Properties preserved under homomorphisms. *Pacific Journal of Mathematics* **9** (1959), pp. 143–154.

70. Lyndon, R. C.: Relation algebras and projective geometries. *Michigan Mathematical Journal* **8** (1961), pp. 21–28.

71. Maddux, R. D.:*Topics in relation algebras*. Doctoral dissertation, University of California at Berkeley, Berkeley CA, 1978, iii + 241 pp.

72. Maddux, R. D.: Some sufficient conditions for the representability of relation algebras. *Algebra Universalis* **8** (1978), pp. 162–172.

73. Maddux, R. D.: Embedding modular lattices into relation algebras. *Algebra Universalis* **12** (1981), pp. 242–246.

74. Maddux, R. D.: Some varieties containing relation algebras. *Transactions of the American Mathematical Society* **272** (1982), pp. 501–526.

75. Maddux, R. D., Pair-dense relation algebras. *Transactions of the American Mathematical Society* **328** (1991), pp. 83–129.

76. Maddux, R. D.: The origin of relation algebras in the development and axiomatization of the calculus of relations. *Studia Logica* **50** (1991), pp. 421–455.

77. Maddux R. D.: Relation-algebraic semantics. *Theoretical Computer Science* **160** (1996), pp. 1–85.

78. Maddux, R. D.: *Relation algebras*. Studies in Logic and the Foundations of Mathematics, vol. 150, Elsevier Science, North-Holland Publishing Company, Amsterdam, 2006, xxvi + 731 pp.

79. Maddux R. D.: Arrow's theorem for incomplete relations. *Journal of Logic and Algebraic Programming* **83** (2014), pp. 235–248.

80. Marx, M.: Relativized relation algebras. *Algebra Universalis* **41** (1999), pp. 23–45.

81. McCoy, N. H.: Subrings of infinite direct sums. *Duke Mathematical Journal* **4** (1938), pp. 486–494.

82. McKenzie, R. N.: *The representation of relation algebras*. Doctoral dissertation, University of Colorado, Boulder CO, 1966, vii + 128 pp.

83. McKenzie, R. N.: Representations of integral relation algebras. *Michigan Mathematical Journal* **17** (1970), pp. 279–287.

84. McKenzie, R. N., McNulty, G. F., and Taylor, W. F.: *Algebras, lattices, varieties*. Volume 1. Wadsworth and Brooks/Cole, Belmont CA, 1987, xvi + 361 pp.

85. McKinsey, J. C. C.: The decision problem for some classes of sentences without quantifiers. *Journal of Symbolic Logic* **8** (1943), pp. 61–76.

86. Monk, J. D.: *Studies in cylindric algebras*. Doctoral dissertation, University of California at Berkeley, Berkeley CA, 1961, vi + 83 pp.

87. Monk, J. D.: On representable relation algebras. *Michigan Mathematical Journal* **11** (1964), pp. 207–210.

88. Peirce, C. S.: Note B. The logic of relatives. In: C. S. Peirce (ed.) *Studies in logic by members of the Johns Hopkins University*, Little, Brown, and Company, Boston, 1883, pp. 187–203. [Reprinted by John Benjamins Publishing Company, Amsterdam, 1983.]

89. Pixley, A. F.: Functionally complete algebras generating distributive and permutable classes. *Mathemamtische Zeitschrift* **114** (1970) pp. 361-372.

90. Riguet, J.: Relations binaires, fermetures, correspondances de Galois. *Bulletin de la Société Mathématique de France* **76** (1948), pp. 114–155.

91. Riguet, J.: Quelques propriétès des relations difonctionnelles. *Comptes Rendus Mathématique de l'Académie des Sciences* **230** (1950), pp. 1999–2000.

92. Russell, B.: *The principles of mathematics.* Cambridge University Press, 1903. [Reprinted by Allen & Unwin, London, 1948.]

93. Sain, I.: Strong amalgamation and epimorphisms of cylindric algebras and Boolean algebras with operators. *Preprint #1982/17*, Mathematical Institute of the Hungarian Academy of Sciences, Budapest, 1982, 44 pp.

94. Sain, I.: Weak products for universal algebra and model theory. *Diagrammes*, vol. 8 (1982), pp. S2–S15.:

95. Schmidt, G.: *Relational mathematics.* Encyclopedia of Mathematics and its Application, vol. 132, Cambridge University Press, Cambridge, 2011, xiii +566 pp.

96. Schmidt, G.: Relational concepts in social choice. In: T. G. Griffin and W. Kahl (eds.) *Relational and algebraic methods in computer science. 13th interational conference on relational and algebraic methods in computer science 2012, Cambridge, UK, September 17–20, 2012. Proceedings*, Lecture Noties in Computer Science, vol. 7650, Springer Verlag, Berlin, 2012, pp. 278–293.

97. Schmidt, G. and Ströhlein, T.: *Relations and graphs—Discrete mathematics for computer scientists.* EATCS Monograph on Theoretical Computer Science, Springer-Verlag, Berlin, 1993, ix + 301.

98. Schröder, E.: *Vorlesungen über die Algebra der Logik (exakte Logik). Dritter Band. Algebra und Logik der Relative. Erste Abteilung.* B. G. Teubner, Leipzig, 1895. [Reprinted by Chelsea Publishing Company, New York, 1966.]

99. Sikorski, R.: Cartesian products of Boolean algebras. *Fundamenta Mathematicae* **37** (1950), pp. 125–136.

100. Sikorski, R.: *Boolean algebras*. Second edition. Ergebnisse der Mathematik und Ihrer Grenzgebiete, vol. 25, Springer-Verlag, Berlin, 1964, x + 237 pp.

101. Skolem, T.: Logisch-kombinatorische Untersuchungen über die Erfüllbarkeit oder Beweisbarkeit mathematischer Sätze nebst einem Theorem über dichte Mengen. *Skrifter utgitt av Videnskapsselskapet i Kristiania, I, Matematisk-naturvidenskabelig klasse* **4** (1920), 36 pp.

102. Tarski, A.: Bemerkung der Redaktion. *Fundamenta Mathematicae* **23** (1934), p. 161.

103. Tarski, A.: Grundzüge des Systemenkalküls. *Fundamenta Mathematicae* **26** (1936), pp. 283–301.

104. Tarski, A.: On the calculus of relations. *Journal of Symbolic Logic* **6** (1941), pp. 73–89.

105. Tarski, A.: Lecture notes on the theory of relation algebras. Taken by B. Jónsson, University of California at Berkeley, some time during the period 1942 to 1945.

106. Tarski, A.: Manuscript of a book containing some of Tarski's early contributions to the theory of relation algebras, written during the period 1943 to 1945. The book was never published, but most of the results in the book were later included in [113].

107. Tarski, A.: Some metalogical results concerning the calculus of relations. *Journal of Symbolic Logic* **18** (1953), pp. 188–189.

108. Tarski, A.: A formalization of set theory without variables. *Journal of Symbolic Logic* **18** (1953), p. 189.

109. Tarski, A.: An undecidable system of sentential calculus.*Journal of Symbolic Logic* **18** (1953), p. 189.

110. Tarski, A.: Contributions to the theory of models, III. *Koninklijke Nederlandse Akademie van Wetenschappen*, *Proceedings*, *Series A*, *Mathematical Sciences* **58** (=*Indagationes Mathematicae* **17**) (1955), pp. 56–64.

111. Tarski, A.: Equationally complete rings and relation algebras. *Koninklijke Nederlandse Akademie van Wetenschappen*, *Proceedings*, *Series A*, *Mathematical Sciences* **59** (=*Indagationes Mathematicae* **18**) (1955), pp. 39–46.

112. Tarski, A.: Lecture notes on the theory of relation algebras. Taken by S. Givant, University of California at Berkeley, 1970.

113. Tarski, A. and Givant, S.: *A formalization of set theory without variables*. Colloquium Publications, vol. 41, American Mathematical Society, Providence RI, 1987, xxi + 318 pp.

114. Tarski, A. and Vaught, R.: Arithmetical extensions of relational systems. *Compositio Mathematica* **13** (1957), pp. 81–102.

115. Weinstein, J. M.: *First-order properties preserved by direct products.* Doctoral dissertation, University of Wisconsin, Madison WI, 1965, 162 pp.

116. Werner, H.: A Mal'cev condition for admissible relations. *Algebra Universalis* **3** (1973), pp. 263.

117. Werner, H.: Diagonal products and affine completeness. *Algebra Universalis* **4** (1974), pp. 269–270.

118. Werner, H.: Congruences on products of algebras and functionally complete algebras. *Algebra Universalis* **4** (1974), pp. 99–105.

119. Werner, H.: *Discriminator algebras.* Studien zur Algebra und ihre Andwendungen, vol. 6, Akademie Verlag, Berlin, 1978.

120. Winter, M.: *Dependencies in relational models of databases.* To appear in: Festschrift J.N. Oliveira of JLAMP, September 01, 2015.

121. Wostner, U.: Finite relation algebras. *Notices of the American Mathematical Society* **23**, (1976), A-482.

122. Zierer, H.: Relation algebraic domain constructions. *Theoretical Computer Science* **87** (1991), pp. 163–188.

.

Index

S. Givant, *Introduction to Relation Algebras*,
DOI 10.1007/978-3-319-65235-1